

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03 –

Специализация -

Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

МОДЕЛЬ УГРОЗ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВЕБ-САЙТА
ПРАВИТЕЛЬСТВА ПЕНЗЕНСКОЙ ОБЛАСТИ

Студент

Елисеев Валерий Витальевич

Руководитель



Елисеев Валерий Витальевич

Комиссарова Н.А.

Нормоконтролёр

Фатеев А.Г.

Рецензент начальник отдела

администрирования и отчётности

Управления цифрового развития,

информационных технологий и связи

Пензенской области



Горин Е.А.

Работа допущена к защите (протокол заседания кафедры от 21.06.19 № 16)

Заведующий кафедрой

С.Л. Зефирова

Работа защищена с отметкой хорошо (протокол заседания ГЭК от 26.06.19 № 30)

Секретарь ГЭК

А.П. Иванов

А.П. Иванов

Пенза 2019

Проверка ВЕР 10.06.19
С.Л. Зефирова

Оглавление

Введение.....	4
1 Выбор и обоснование актуальности темы выпускной квалификационной работы.....	6
2 Анализ законодательства Российской Федерации и Пензенской области в сфере обеспечения безопасности персональных данных и информационных систем общего пользования.....	8
2.1 Основные документы, регламентирующие порядок обеспечения безопасности персональных данных.....	8
2.2 Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».....	10
2.3 Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».....	12
2.4 Основные документы, регламентирующие порядок защиты информационных систем общего пользования.....	14
3 Описание информационной системы «Веб-сайт Правительства Пензенской области».....	15
4 Идентификация активов и определение их ценности.....	22
5 Описание информационной системы и особенностей её функционирования.....	26
5.1 Назначение ИС.....	26
5.2 Исходные данные об ИС.....	26
5.3 Описание структурно-функциональных характеристик.....	27
6 Типы и виды нарушителей, их возможный потенциал (модель нарушителя).....	29
7 Определение актуальных угроз	35

7.1	Определение уровня исходной защищённости.....	35
7.2	Оценка степени возможного ущерба от реализации угрозы безопасности информации.....	36
7.3	Определение актуальности угрозы безопасности информации.....	40
8	Возможность использования разработанной модели угроз информационной системы «Веб-сайта Правительства Пензенской области» для идентификации актуальных угроз информационных систем веб-сайтов исполнительных органов государственной власти и органов местного самоуправления Пензенской области.....	162
9	Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	165
	Заключение.....	168
	Список использованных источников.....	169
	Приложение А Перечень информационных и вспомогательных активов информационной системы «Веб-сайт Правительства Пензенской области»...	172
	Приложение Б Акт классификации информационной системы «Веб-сайт Правительства Пензенской области».....	175
	Приложение В Модель нарушителя.....	180
	Приложение Г Модель угроз.....	190

Введение

Обеспечение безопасности информационных систем персональных данных и информационных систем общего пользования крайне трудоёмкая задача, отчасти потому, что разработкой самой системы зачастую занимаются люди не сведущие в особенностях создания защищённых систем. В такие моменты и необходимы специалисты по информационной безопасности, вся работа которых начинается именно с исследования информационной системы.

Процесс создания информационной системы в защищённом исполнении крайне сложен и состоит из множества этапов, среди которых особое место занимает этап создания модели нарушителя и модели угроз потому, что именно от того, насколько точно будут созданы данные модели, зависит эффективность принимаемых защитных мер.

Для того, чтобы обеспечить достойную защиту информационной системы необходимо для начала изучить рассматриваемую систему, рассмотреть информационные процессы, которые в ней происходят, персонал, который взаимодействует с данной системой, и многое другое. Именно поэтому на первом этапе данной работы производится описание информационной системы а также анализ информационных активов. На основании информации, полученной на первом этапе производится анализ системы с целью создания модели нарушителя и модели угроз и лишь после всего перечисленного производится создание модели угроз.

Целью выпускной квалификационной работы является изучение информационной системы «Веб-сайт Правительства Пензенской области» с целью создания модели нарушителей и модели угроз информационной безопасности. Также в данной работе рассматривается возможность использования созданных моделей в аналогичных государственных информационных системах. В завершение преддипломной практики производится создание следующих документов: перечень информационных и

вспомогательных активов, акт классификации, модель угроз и модель нарушителя информационной системы.

1 Выбор и обоснование актуальности темы выпускной квалификационной работы

Современный мир просто невозможно представить без использования информационных технологий, несмотря на то, что их повседневное применение началось лишь в начале 21 века, за это короткое время они прочно укоренились во всех областях жизни, и с каждым днём их влияние растёт. Информационные технологии позволяют упростить многие процессы жизнедеятельности в различных сферах жизни.

Человек - существо социальное, и особое место в жизни любого индивидуума играет государство и социум. Раньше человек узнавал о деятельности государственного аппарата при помощи газет, радиовещания, а все государственные услуги получал в специализированных учреждениях. Но время идёт, и сейчас для граждан нашей страны создаются специализированные информационные системы, способные упростить получение необходимой информации, уменьшить количество бумажных документов а также значительно упростить процесс хранения бумажной документации. Помимо всего прочего граждане, которые не могли раньше в силу определённых трудностей обратиться лично с вопросами к государственным служащим, получают возможность обратиться к ним удалённо, при помощи сети интернет.

Но наряду с несомненными достоинствами, есть и существенные недостатки внедрения информационных систем так, например возможность нарушения свойств конфиденциальности, целостности и доступности информации, обрабатываемой в системе может нанести значительный ущерб государственному органу вплоть до невозможности выполнения своих функций. Также ни одна информационная систем не способна функционировать без аппаратных средств, поэтому им также как и информации необходима соответствующая защита.

Одной из таких информационных систем является - «Веб-сайт Правительства Пензенской области», данный ресурс позволяет гражданам получать необходимую информацию о деятельности Правительства Пензенской области, а также получать доступ к государственным услугам в электронном виде. Вследствие этого возникает необходимость в защите персональных данных пользователей данной системы, а также информационной составляющей данного ресурса, ведь в случае изменения информации на данном ресурсе возникает возможность дискредитации деятельности Правительства Пензенской области.

Модель угроз — документ, использующийся для установления возможности нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, а также позволяющий установить, приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора.

Модель угроз — одна из важнейших составляющих в процессе защиты информационной системы, именно от того, насколько досконально она будет создана, во много зависит эффективность всего процесса защиты. Именно поэтому темой данной выпускной квалификационной работы стала «Модель угроз для информационной системы веб-сайта Правительства Пензенской области».

2 Анализ законодательства Российской Федерации и Пензенской области в сфере обеспечения безопасности персональных данных и информационных систем общего пользования

2.1 Основные документы, регламентирующие порядок обеспечения безопасности персональных данных

Защита персональных данных в государственных информационных системах Пензенской области, осуществляется в соответствии с действующим законодательством Российской Федерации, а именно:

— Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»[1];

— постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

— постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»[3];

— приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

— приказом ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

— приказом ФСТЭК России от 15 февраля 2017 года № 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

— приказом ФСБ России от 10 июля 2014 года № 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 5 криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

— «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 15 февраля 2008 года;

— «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 14 февраля 2008 года;

— «Моделью угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли», согласованная с ФСТЭК России, ФСБ России и одобренная Решением секции № 1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» от 21 апреля 2010 года № 2;

— постановлением Правительства Российской Федерации от 11.05.2017 N 555 «О внесении изменений в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;

— другими актами, определяющими политику Российской Федерации и Пензенской области в сфере защиты информации.

Далее был произведён анализ федеральных законов и постановлений правительства, методики и приказы ФСТЭК и ФСБ России рассмотрены не будут из-за объёма.

2.2 Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»

Данный федеральный закон регулирует отношения, возникающие при обработке персональных данных. В нашем случае ФЗ рассматривается относительно органов местного самоуправления, которые попадают в сферу действия данного закона. Особое внимание стоит уделить следующему: «Действие настоящего Федерального закона не распространяется на отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну» [1].

Особое внимание при организации обработки персональных данных стоит уделить принципам обработки персональных данных. Так среди них стоит в первую очередь выделить:

«3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и

актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.»

Согласно третьему пункту объединение разных баз данных, несовместимых между собой является неприемлемым, даже если при этом существенно уменьшится количество задействованных ресурсов.

Согласно шестому пункту оператор должен своими действиями способствовать уточнению данных, получаемых в процессе работы. Данный пункт имеет огромную ценность так как лишь при правильной работе оператора в базе данных будут присутствовать необходимые для работы данные в полном объёме, а также отсутствовать избыточность данных.

В статье 6 данного федерального закона рассматриваются условия обработки персональных данных. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. Но тут стоит отметить что обработка персональных данных не требует согласия, если обработка необходима в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, необходима для исполнения судебного акта, необходима для исполнения полномочий федеральных органов исполнительной власти, обработка персональных данных необходима для защиты жизни и здоровья субъекта и другое.

Также стоит выделить пункт 4: «Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных»

Это означает, что для обработки данных субъекта достаточно получить его согласие лишь оператором, при дальнейшей обработке согласие не требуется а всю ответственность перед субъектом персональных данных несет оператор.

Особое внимание стоит уделить статье 19 — меры по обеспечению безопасности персональных данных при их обработке.

В данной статье описаны основные принципы по обеспечению безопасности персональных данных при их обработке а также действия, применяемые сотрудниками для обеспечения безопасности персональных данных.

Так оператор обязан принимать необходимые меры по обеспечения защиты персональных данных, препятствовать их неправомерному удалению, изменению, копированию, распространению.

Обобщая выделенные моменты из данного федерального закона, получается, что данный ФЗ регулирует процесс обращения с персональными данными в органах местного самоуправления, указывает персональные данные, на которые распространяется данный закон и порядок доступа к ним. Особое место уделено обязанностями оператора и его правам, в частности порядку защиты персональных данных оператором.

2.3 Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Целью данного документа является «Установление требований к защите персональных данных при их обработке в информационных системах персональных данных»[2].

В данном постановлении указывается лицо, ответственное за обеспечении безопасности персональных данных при обработке, так зачастую это оператор. Если оператор передаёт обработку данных другому лицу, тогда с данным лицом должен быть заключен договор и ответственность перед лицом, персональные данные которого обрабатываются несёт оператор, а лицо, заключившее договор на обработку персональных данных несёт ответственность перед оператором.

Согласно данному постановлению устанавливаются несколько типов информационных систем:

- информационная система, обрабатывающая специальные категории персональных данных;
- информационная система, обрабатывающая биометрические персональные данные;
- информационная система, обрабатывающая общедоступные персональные данные;
- информационная система, обрабатывающая иные категории персональных данных;
- информационная система, обрабатывающая персональные данные сотрудников оператора.

А также устанавливается несколько типов актуальности угроз. Так к угрозам первого типа относятся угрозы связанные с наличием недокументированных возможностей в системном ПО, используемом в системном ПО, угрозы второго типа — наличие недокументированных возможностей в прикладном ПО, используемом в информационной системе, а третьего типа не связанные с недеklarированными уязвимостями в прикладном и системном обеспечении.

В данном постановлении не описывается порядок определения типа угроз безопасности персональных данных, а лишь указывается что он проводится с учётом оценки возможности вреда, порядок проведения которой указан в ФЗ «О персональных данных».

В данном постановлении устанавливаются 4 уровня защищённости персональных данных, условия отнесения персональных данных к определённому уровню, а также требования, обеспечение которых необходимо при отнесении персональных данных к данным уровням.

2.4 Основные документы, регламентирующие порядок защиты информационных систем общего пользования

Решением Координационного Совета по защите информации при полномочном представителе Президента РФ в Приволжском федеральном округе от 24 октября 2017 года предусмотрено исполнение следующих требований требований:

— Приказ ФСБ РФ N 416, ФСТЭК РФ N 489 от 31.08.2010 Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования[5];

— Приказ Минкомсвязи РФ от 25.08.2009 N 104 Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования[6];

— Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[7];

— Постановление Правительства РФ от 18 мая 2009 г. N 424 "Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям".

3 Описание информационной системы «Веб-сайт Правительства Пензенской области»

Была выделена целевая функция информационной системы «Веб-сайт Правительства Пензенской области». В качестве целевой функции системы была выделена обеспечение реализации прав граждан по получению государственных и муниципальных услуг в электронном виде.

Было принято решение составить описание процессов, необходимых для выполнения целевой функции системы, в виде диаграмм, используя методологию функционального моделирования IDEF0.

Были определены взаимосвязи проектируемой ИС с внешней средой, после чего было составлено описание целевой функции системы. Описание целевой функции системы было представлено в виде диаграммы, приведенная на рисунке 1.

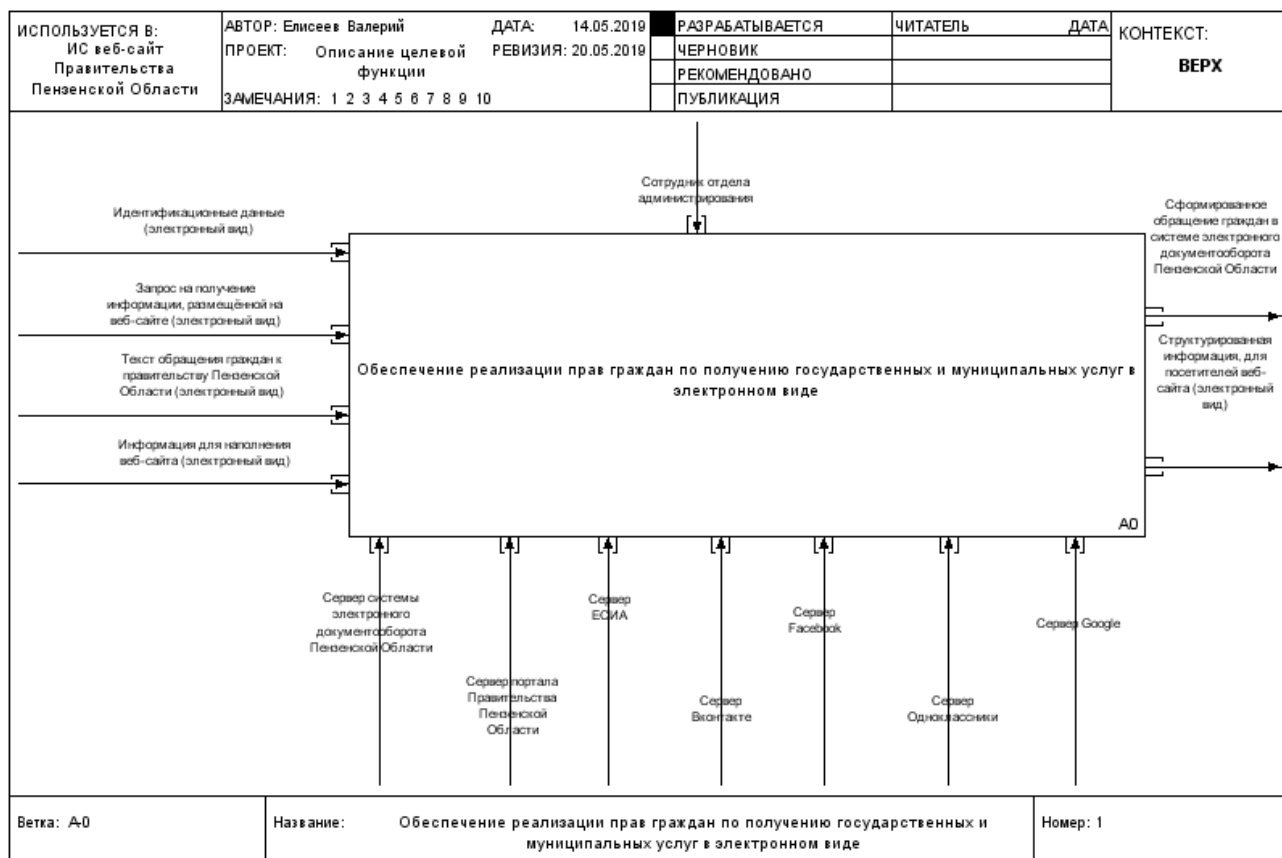


Рисунок 1 — Описание целевой функции

Для детального описания процессов, необходимых для выполнения целевой функции системы, была проведена ее декомпозиция с помощью методологии функционального моделирования IDEF0. Результат декомпозиции был представлен в виде диаграммы A0, приведенной на рисунке 2.

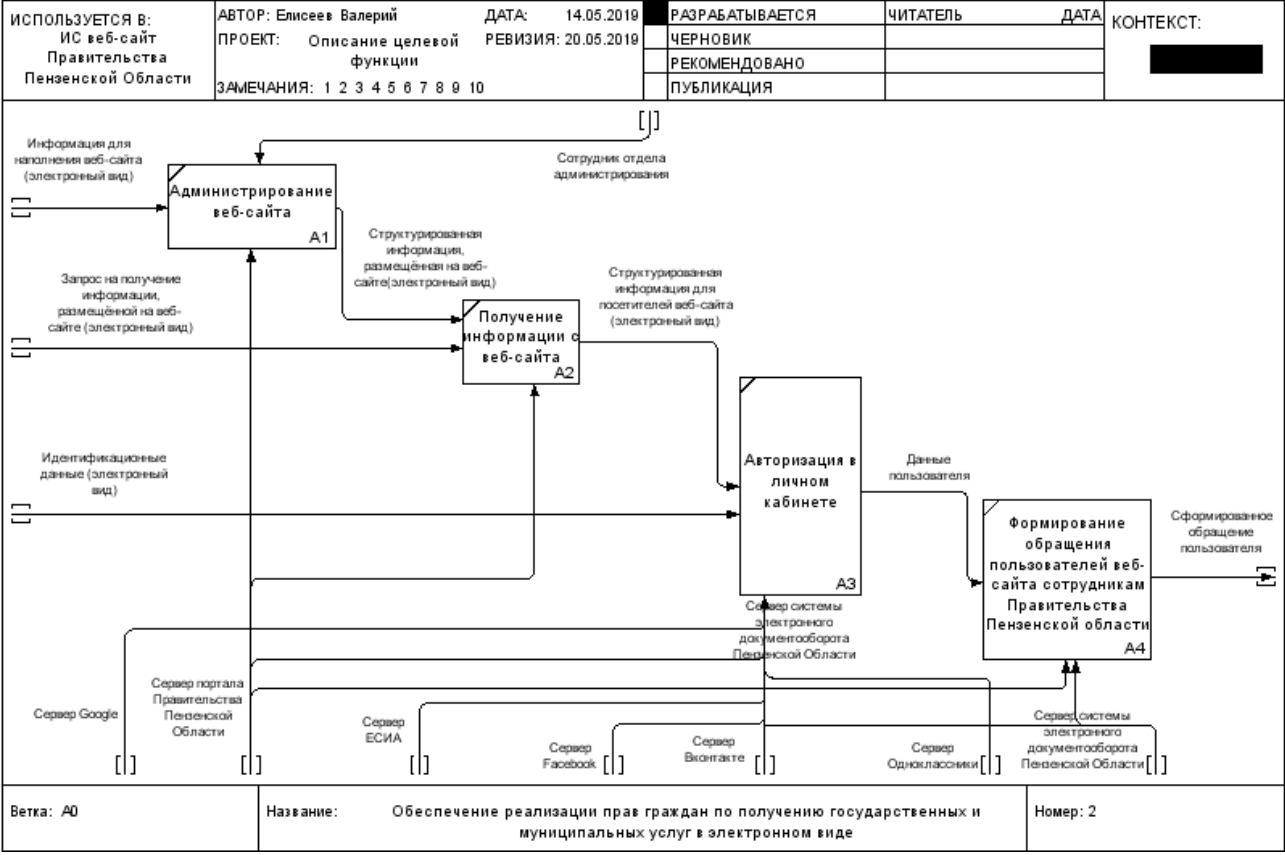


Рисунок 2 — Декомпозиция целевой функции

Было принято решение построить частные инфологические модели для информационных процессов, полученных в результате декомпозиции целевой функции системы, и представить их в виде направленных графов.

Было принято решение отмечать на ребрах графов в рамках инфологических моделей критичность информационного потока и предполагаемый объем данных согласно таблице 1.

Таблица 1 — Условные обозначения критичности и объема потока

	Высокий уровень	Средний уровень	Низкий уровень
Критичность потока	В	С	Н
Объем потока	3	2	1

Были составлены частные инфологические модели процессов «Администрирование веб-сайта», «Получение информации с веб-сайта», «Авторизация в личном кабинете» и «Формирование обращения пользователей веб-сайта сотрудникам Правительства Пензенской области». Полученные инфологические модели представлены на рисунках 3,4,5 и 6 соответственно.

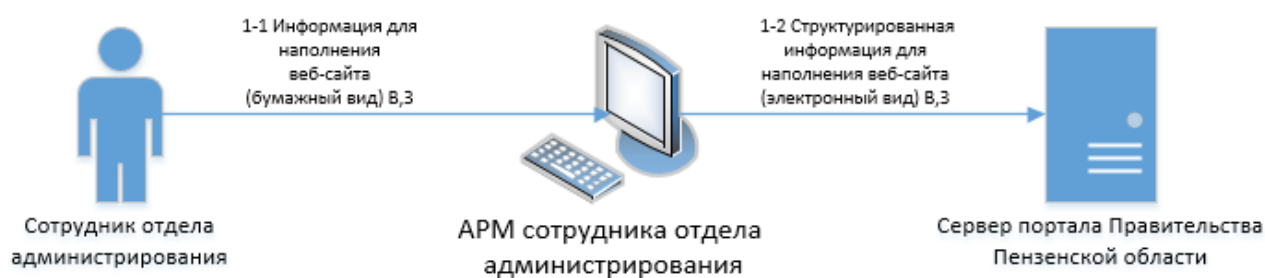


Рисунок 3 — Частная инфологическая модель процесса администрирования веб-сайта

Для администрирования веб-сайта сотрудник по подготовленной информации формирует блоки данных, которые заносятся на веб-страницу при помощи АРМ сотрудника, расположенного на территории организации.



Рисунок 4 — Частная инфологическая модель процесса «Получение информации с веб-сайта»

Информация, размещённая на веб-сайте Правительства Пензенской области передаётся по сети интернет, после соответствующего запроса с АРМ

пользователя. Для получения информации, пользователю не нужно быть авторизованным на веб-сайте.

Для формирования обращения сотрудникам Правительства Пензенской области, пользователю необходимо авторизоваться на веб-сайте при помощи учётной записи одного из следующих сервисов: почтовый клиент «Google», социальная сеть «Одноклассники», социальная сеть «ВКонтакте», социальная сеть «Facebook» либо при помощи «Единой системы идентификации и аутентификации». При авторизации пользователь отсылается на соответствующий ресурс, где проходит процедуру аутентификации и по её результатам на веб-сайт Правительства Пензенской области поступают идентификационные данные пользователя.

При формировании обращения сотрудникам Правительства Пензенской области, пользователь составляет обращение и размещает его на веб-сайте Правительства Пензенской области, откуда оно передаётся на сервер электронного документооборота Пензенской области.

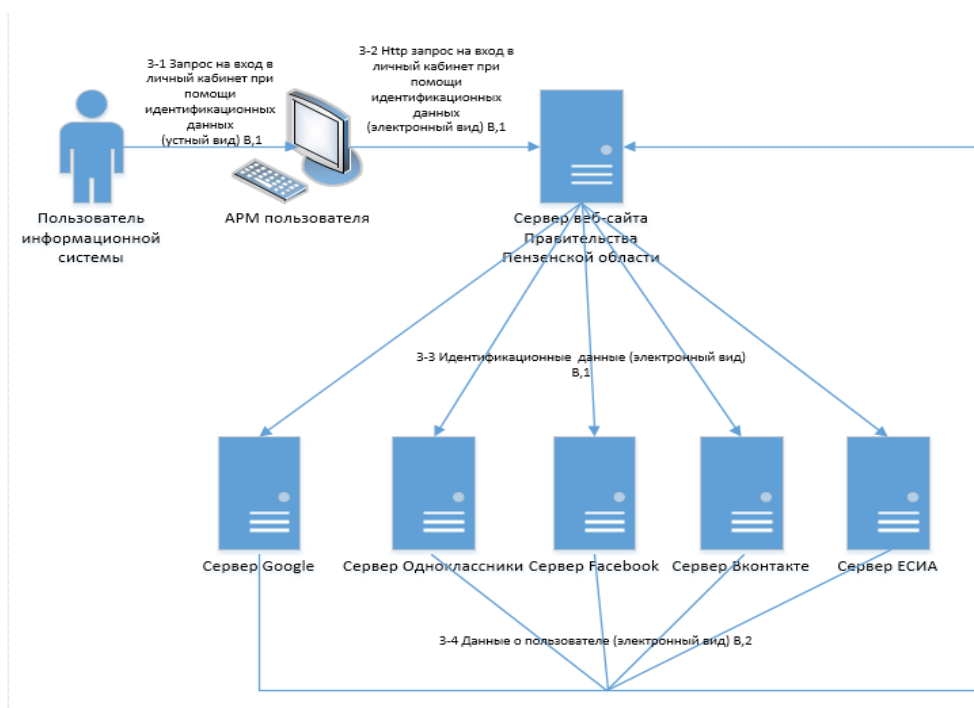


Рисунок 5 — Частная инфологическая модель процесса «Авторизация в личном кабинете»

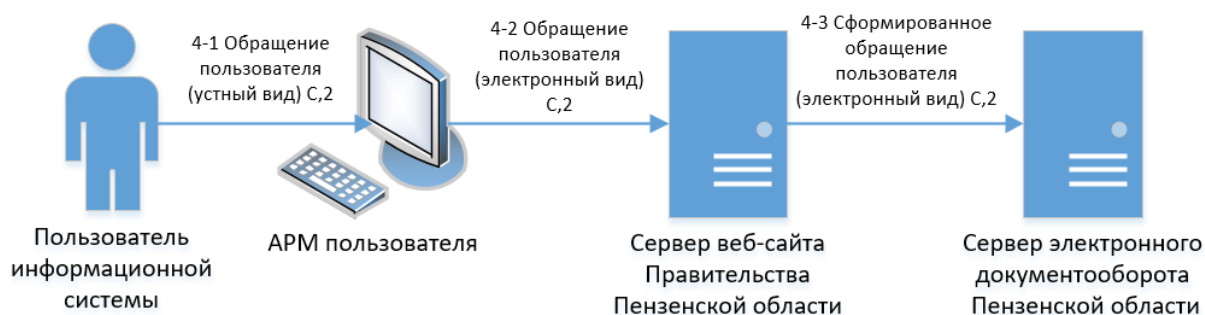


Рисунок 6 — Частная инфологическая модель процесса «Формирование обращения пользователей веб-сайта сотрудникам Правительства Пензенской области»

Была построена общая инфологическая модель ИС, представленная на рисунке 7.

Описание информационных потоков, изображенных на общей инфологической модели ИС «Веб-сайт правительства Пензенской области», приведено в таблице 2.

Таблица 2 — Описание информационных потоков

Идентификатор	Описание	Параметры
1 - 1	Информация для наполнения веб-сайта (бумажный вид)	В, 3
1 - 2	Структурированная информация для наполнения веб-сайта (электронный вид)	В, 3
2 - 1	Запрос на получение информации, размещённой на веб-сайте (устная форма)	Н, 1
2 - 2	Http запрос к серверу на получение информации, размещённой на веб-сайте (электронный вид)	Н, 1
3 - 1	Запрос на вход в личный кабинет при помощи идентификационных данных (устный вид)	В, 1
3 - 2	Http запрос на вход в личный кабинет при помощи идентификационных данных (электронный вид)	В, 1
3 - 3	Идентификационные данные (электронный вид)	В, 1
3 - 4	Данные о пользователе (электронный вид)	В, 2
4 - 1	Обращение пользователя(устный вид)	С, 2
4 - 2	Обращение пользователя (электронный вид)	С, 2
4 - 3	Сформированное обращение пользователя (электронный вид)	С, 2

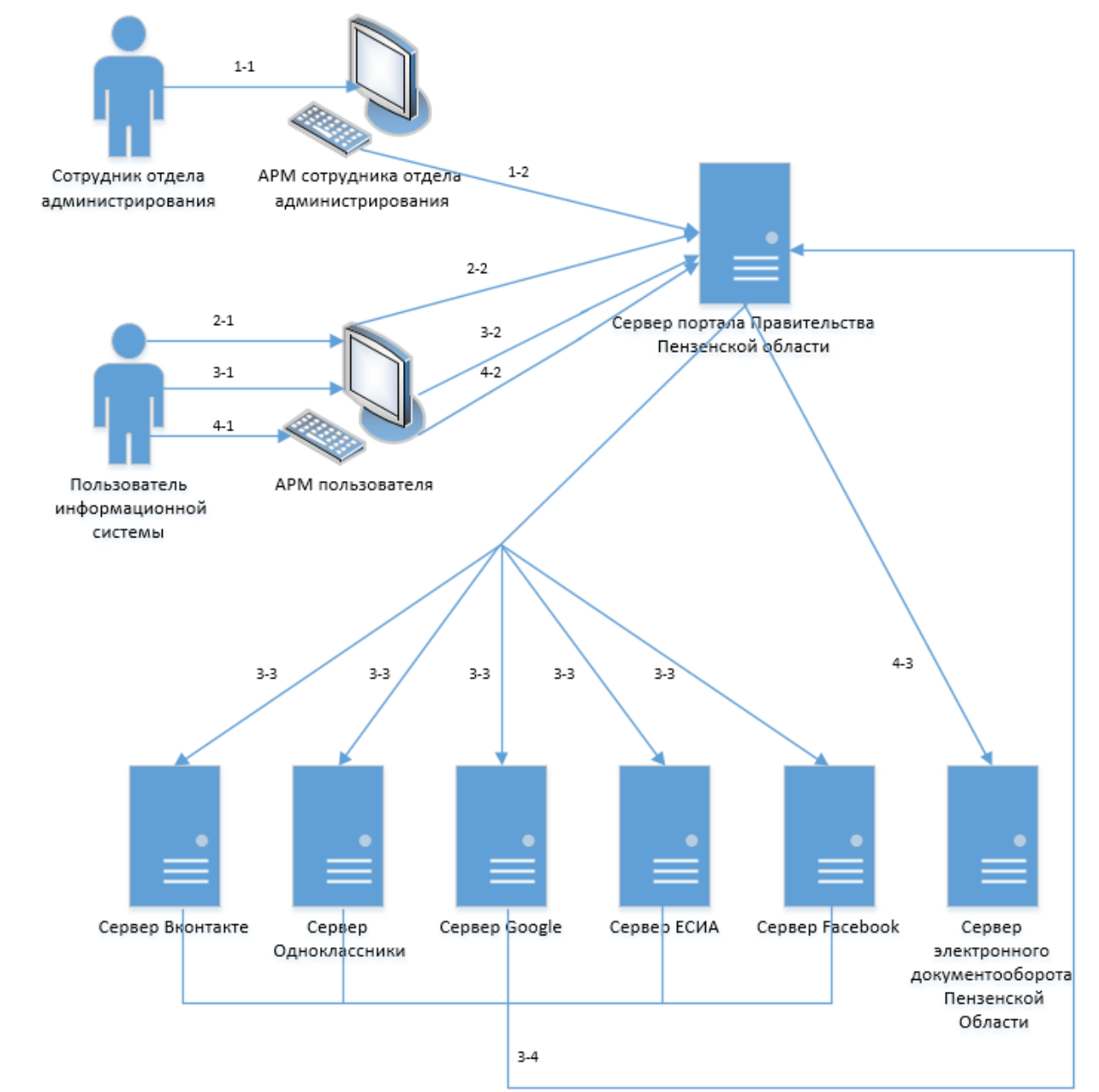


Рисунок 7 — Общая инфологическая модель ИС организации

Структурная модель ИС «Веб-сайт Правительства Пензенской области», описывающая также компонентный состав ИС, представлена на рисунке 8.

Перечень материальных активов и их стоимость указаны в таблице 3.

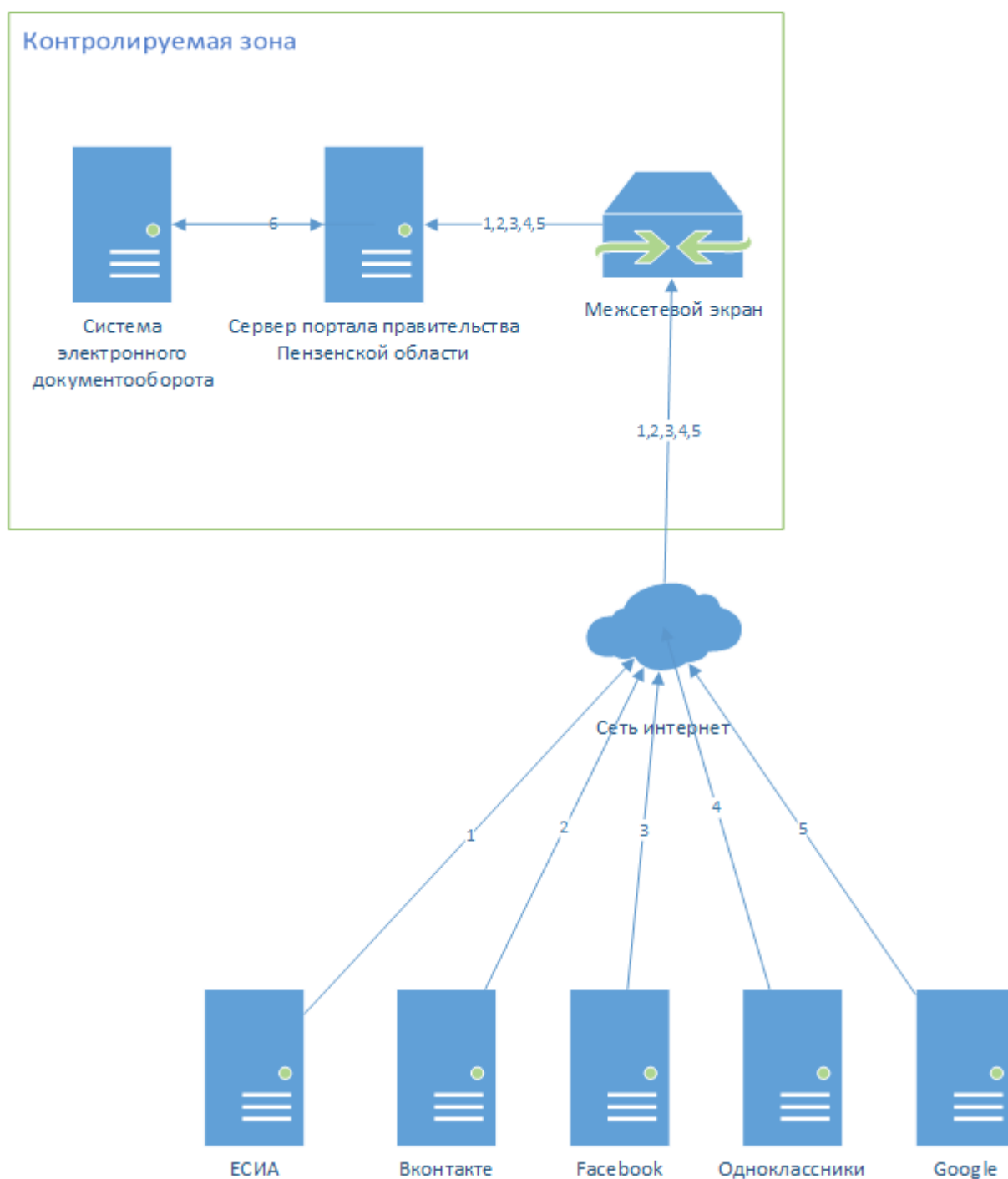


Рисунок 8 — Структурная модель ИС

Таблица 3 – Стоимость материальных активов

Наименование компонента	Цена за единицу, руб	Количество	Стоимость, руб
Сервер HPE ProLiant DL560	2505880	2	5011760
АРМ сотрудника отдела администрирования IRU Office S2301	33530	2	67060
Межсетевой экран ZYXEL ZyWALL USG 1000	27535	1	27535
Среда виртуализации Oracle VM VirtualBox Enterprise	61746	1	61746
Коммутатор D-LINK DGS-3620-28SC/B1AEI	159440	1	159440

4 Идентификация активов и определение их ценности

Был определен перечень активов информационной системы «Веб-сайт Правительства Пензенской области». Был установлен следующий перечень типов защищаемых активов информационной системы:

- информационные активы;
- бизнес-процессы;
- аппаратные средства;
- программные средства;
- персонал организации.

К информационным были отнесены следующие активы:

- персональные данные клиентов ИС;
- служебная информация;
- обращения граждан;
- идентификационные данные клиентов ИС.

К вспомогательным были отнесены следующие активы:

- АРМ сотрудников (2 шт.);
- сетевое оборудование;
- сервер веб-сайта правительства Пензенской области;
- сервер системы электронного документооборота Пензенской области;
- среда виртуализации Oracle VM VirtualBox Enterprise.

Был определен перечень значимых свойств информации, обрабатываемой в информационной системе. Такими свойствами были признаны конфиденциальность, доступность и целостность. Была определена принадлежность значимых свойства ИБ каждому информационному активу информационной системы. Результат представлен в таблице 4.

Таблица 4 – Перечень информационных активов и их значимых свойств ИБ

Информационный актив	Значимые свойства ИБ		
	Конфиденциальность	Целостность	Доступность
Персональные данные клиентов ИС	+	+	+
Служебная информация	-	+	-
Обращения граждан	+	+	-
Идентификационные данные клиентов ИС	+	+	+

Для установленных критериев влияния была введена нумерация в соответствии с таблицей 5.

Таблица 5 – Нумерация критериев влияния

№ критерия	Название критерия
1	Критерий нарушения непрерывности деятельности организации
2	Критерий финансовых и материальных потерь
3	Критерий затрат дополнительных людских ресурсов
4	Критерий потери времени на ремонт, замену или восстановление актива
5	Критерий нарушения законодательных или договорных требований

По заданным критериям влияния было проведено оценивание величины нарушений ИБ для каждого информационного актива, результаты представлены в таблице 6.

В таблице были введены следующие сокращения:

- К – конфиденциальность;
- Д – доступность;
- Ц – целостность;
- НЛ – нулевой уровень;
- Н – низкий уровень;
- С – средний уровень;
- В – высокий уровень.

Таблица 6 – Результаты оценивания величин нарушения ИБ

Информационный актив	Свойства ИБ	Оценка нарушения ИБ					Обобщенная оценка
		1	2	3	4	5	
Персональные данные клиентов ИС	К	В	В	НЛ	Н	В	В
	Д	С	НЛ	НЛ	С	НЛ	С
	Ц	С	НЛ	НЛ	С	НЛ	С
Идентификационные данные клиентов ИС	К	С	В	НЛ	НЛ	В	В
	Д	С	НЛ	НЛ	НЛ	С	С
	Ц	С	НЛ	НЛ	НЛ	С	С
Обращения граждан	К	Н	НЛ	НЛ	Н	С	С
	Д	С	НЛ	НЛ	С	С	С
	Ц	С	НЛ	НЛ	С	С	С

Продолжение таблицы 6

Информационный актив	Свойства ИБ	Оценка нарушения ИБ					Обобщенная оценка
Служебная информация	К	Н	НЛ	НЛ	НЛ	Н	Н
	Д	С	НЛ	С	С	С	С
	Ц	С	НЛ	С	С	С	С

Обобщенная качественная оценка величины нарушения ИБ была определена на основании результатов оценивания величины нарушений ИБ для каждого информационного актива. Она была определена как максимальная (наиболее тяжелая) оценка величины нарушения ИБ, полученная по направлениям оценивания.

Была определена ценность вспомогательных активов исходя из их стоимости, а также ценности зависимых от них информационных активов. Критерии оценивания вспомогательных активов представлены в таблице 7.

Таблица 7 – Критерии определения стоимости вспомогательных активов

Стоимость	Критерии, определяющие величину стоимости
Минимальная	Затраты на приобретение и поддержку актива составляют незначительную часть бюджета организации. Дополнительные средства для их восстановления не требуются.
Низкая	Затраты на приобретение и поддержку актива составляют существенную часть бюджета организации. Для восстановления поврежденного актива могут потребоваться дополнительные средства.
Средняя	Затраты на приобретение и поддержку актива составляют большую часть бюджета организации. Для восстановления поврежденного актива могут потребоваться сверхплановые финансовые и материальные затраты из бюджета организации.
Высокая	Затраты на приобретение и поддержку актива составляют большую часть бюджета организации. Для восстановления поврежденного актива могут потребоваться сверхплановые финансовые и материальные затраты, объем которых не может быть покрыт бюджетом организации, вследствие чего потребуются привлечение финансовых и материальных средств со стороны.

С помощью матрицы были установлены зависимости между активами, результат представлен в таблице 8.

Результаты оценивания вспомогательных активов представлены в таблице 9. В таблице были введены следующие сокращения:

- МИН – минимальная ценность;
- Н – низкая ценность;
- С – средняя ценность;

— В – высокая ценность.

Таблица 8 – Матрица зависимостей между активами организации

	Вспомогательные активы				
	АРМ сотрудников	Сетевое оборудование	Сервер Веб-сайта правительства Пензенской области	Сервер системы электронного документооборота Пензенской области	Среда виртуализации Oracle VM VirtualBox Enterprise
Зависимые активы					
Персональные данные клиентов ИС	-	+	+	+	+
Идентификационные данные клиентов ИС	-	+	+	-	+
Обращения граждан	-	+	+	+	+
Служебная информация	+	+	-	+	+

Таблица 9 – Ценность вспомогательных активов

Вспомогательные активы	Ценность актива без учета зависимостей	Зависимые активы		Ценность актива с учетом зависимостей
		Информационный актив	Ценность	
АРМ сотрудников	Н	Служебная информация	С	С
Сетевое оборудование	С	Персональные данные клиентов ИС	В	В
		Идентификационные данные клиентов ИС	В	
		Обращения граждан	С	
		Служебная информация	С	
Сервер Веб-сайта правительства Пензенской области	В	Персональные данные клиентов ИС	В	В
		Идентификационные данные клиентов ИС	В	
		Обращения граждан	С	
Сервер системы электронного документооборота Пензенской области	В	Персональные данные клиентов ИС	В	В
		Обращения граждан	С	
		Служебная информация	С	
Среда виртуализации Oracle VM VirtualBox Enterprise	С	Персональные данные клиентов ИС	В	В
		Идентификационные данные клиентов ИС	В	
		Обращения граждан	С	
		Служебная информация	С	

Результаты идентификации и оценки ценности информационных активов приведены в перечне активов, представленного в приложении А.

5 Описание информационной системы и особенностей её функционирования

5.1 Назначение ИС

Информационная система "Веб-сайт Правительства, Пензенской области" предназначена для:

- содействие обеспечению реализации прав граждан (физических лиц) и организаций на доступ к информации о деятельности государственных органов;
- создание дополнительных условий и сервисов для взаимодействия Правительства Пензенской области с физическими лицами, юридическими лицами, органами государственной власти и органами местного самоуправления муниципальных образований Пензенской области;
- формирование единого информационного ресурса, содержащего достоверную информацию о деятельности Губернатора Пензенской области и Правительства Пензенской области;
- совершенствование процедур предоставления государственных услуг в электронном виде, повышение их качества и доступности.

5.2 Исходные данные об ИС

Структура информационной системы: Информационная система состоящая из 1 сервера, подключенного к сети интернет при помощи национального провайдера цифровых сервисов ПАО «Ростелеком».

Цели обработки ПДН: обеспечение реализации прав граждан по получению государственных и муниципальных услуг в электронном виде

Тип обрабатываемых ПДН: общедоступные и иные персональные данные

Количество обрабатываемых ПДН: более чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.

Наличие подключений ИС к сетям связи общего пользования и (или) сетям международного информационного обмена: ИС имеет односторонний выход в сеть Интернет.

Режим обработки персональных данных: Многопользовательская система

Режим разграничения прав доступа пользователей информационной системы: ИС с разграничением прав доступа.

Местонахождение технических средств информационной системы: В пределах РФ: – на мощностях интернет-провайдера ПАО «Ростелеком», а также 440025, г.Пенза, ул.Московская, д.75

Акт классификации ИС «Веб-сайт Правительства Пензенской области» представлен в Приложении Б.

5.3 Описание структурно-функциональных характеристик

Возможные способы реализации угроз зависят от структурно-функциональных характеристик и особенностей информационной системы. Поэтому производится анализ характеристик системы и адаптация рассматриваемого перечня угроз. Из числа рассматриваемых угроз исключаются угрозы, для которых отсутствует сценарий реализации.

Инфологическая схема работы системы представлена на рисунке 1.

В таблице 10 приведено описание информационных потоков, отражённых на рисунке 9.

Таблица 10 — Описание информационных потоков

№ Информационного потока	Описание потока
1	Авторизация при помощи ЕСИА, взаимодействие с порталом государственных услуг
2	Авторизация при помощи сервиса Вконтакте

Продолжение таблицы 10

№ Информационного потока	Описание потока
3	Авторизация при помощи сервиса Facebook
4	Авторизация при помощи сервиса Одноклассники
5	Взаимодействие с порталом kremlin.ru
6	Взаимодействие с региональным порталом государственных услуг
7	Передача обращений граждан в систему электронного документооборота, а также получение ответа на обращения

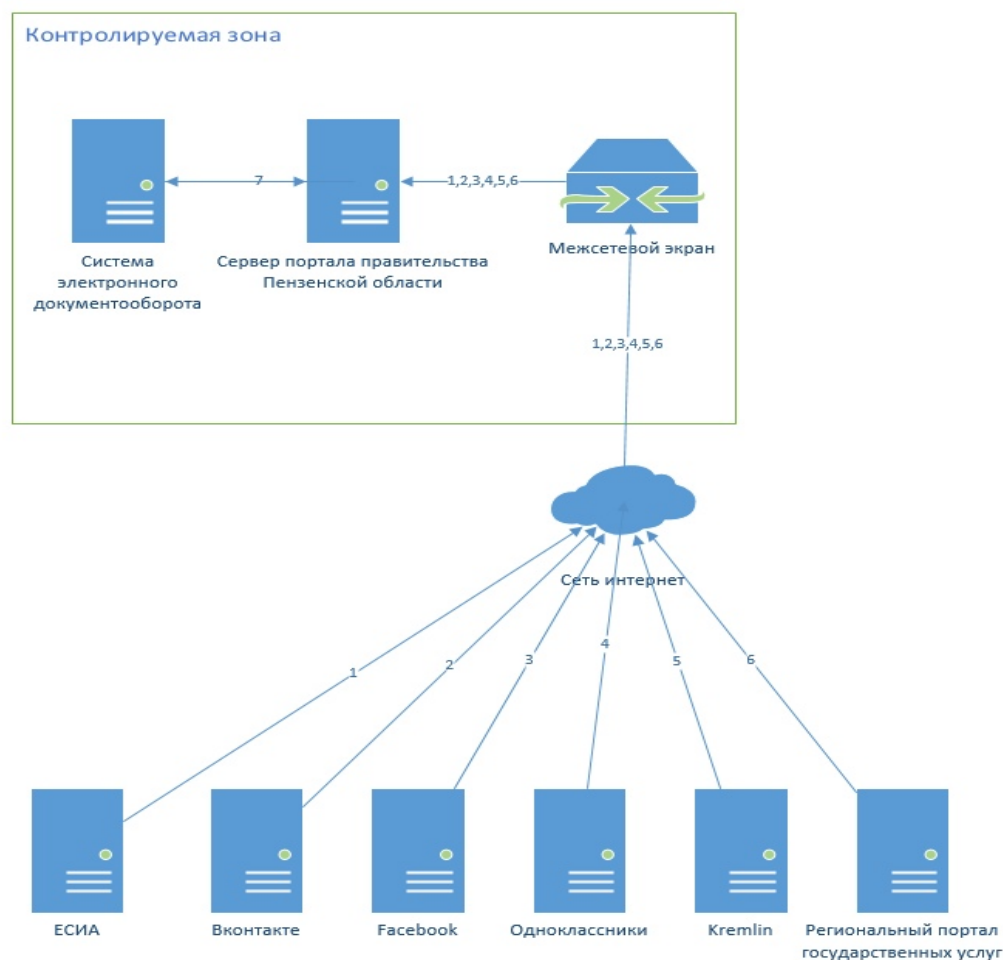


Рисунок 9 — Инфологическая схема информационной системы

6 Типы и виды нарушителей, их возможный потенциал (модель нарушителя)

Основываясь на описании информационной системы и особенностей её функционирования, полученных ранее была сформирована модель нарушителя.

Антропогенными источниками угроз являются нарушители. Потенциальные нарушители характеризуются типом и потенциалом. Тип нарушителя может быть внешним или внутренним.

Тип нарушителя зависит от наличия у него доступа к информационной системе и в контролируемую зону. Внешние нарушители не имеют права доступа к информационной системе и реализуют угрозы из-за границ контролируемой зоны. Внутренние нарушители имеют право постоянного или разового доступа в контролируемую зону.

Потенциал нарушителя характеризует уровень его компетентности, наличия ресурсов и мотивации. Потенциал может быть низким, средним или высоким. Описание нарушителей, их возможной мотивации и предполагаемых возможностей приведено в таблице 11.

Таблица 11 — Описание нарушителей, их возможной мотивации и предполагаемых возможностей

Нарушители	Категория нарушителей	Потенциал нарушителя	Возможная мотивация	Предполагаемые возможности
Лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора	Внутренний	С низким потенциалом	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему

Продолжение таблицы 11

Нарушители	Категория нарушителей	Потенциал нарушителей	Возможная мотивация	Предполагаемые возможности
Пользователи информационной системы	Внешний	С низким потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
Бывшие работники	Внешний	С низким потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
Лица, привлекаемые для установки, наладки, монтажа, пуска и обслуживания и иных работ	Внешний	С низким потенциалом	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему

Продолжение таблицы 11

Нарушители	Категория нарушителей	Потенциал нарушителей	Возможная мотивация	Предполагаемые возможности
Террористические, экстремистские группировки	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы
Разработчики, производители, поставщики и программных, технических и программнотехнических средств	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или некомпетентные действия	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Продолжение таблицы 11

Нарушители	Категория нарушителей	Потенциал нарушителей	Возможная мотивация	Предполагаемые возможности
Администраторы информационной системы и администраторы безопасности	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы
Преступные группы (криминальные структуры)	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Продолжение таблицы 11

Нарушители	Категория нарушителей	Потенциал нарушителя	Возможная мотивация	Предполагаемые возможности
Специальные службы иностранных государств (блоков государств)	Внешний, внутренний	Нарушители с высоким потенциалом	Дискредитация или дестабилизация деятельности органов государственной власти, нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики.	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений

Для рассматриваемой информационной системы отсутствуют следующие нарушители:

— конкурирующие организации, так как в данной сфере конкуренции не существует;

— внешние субъекты, так как в рассматриваемой системе по определению все внешние субъекты взаимодействующие с системой являются пользователями.

Модель нарушителя в виде документа представлена в приложении В.

7 Определение актуальных угроз

7.1 Определение уровня исходной защищённости

Для оценки возможности реализации угрозы применяются два показателя:

- уровень исходной защищённости ИС;
- частота (вероятность) реализации рассматриваемой угрозы.

В ходе эксплуатации информационной системы уровень ее защищенности (Y1) определяется следующим образом:

а) в информационной системе обеспечивается высокий уровень защищенности (Y1), если в ходе эксплуатации информационной системы не появились дополнительные угрозы безопасности информации или в отношении появившихся дополнительных угроз безопасности информации с высокой оперативностью («за минуты») могут быть приняты меры защиты информации, нейтрализующие эти угрозы;

б) в информационной системе обеспечивается средний уровень защищенности (Y1), если в ходе эксплуатации информационной системы появились дополнительные угрозы безопасности информации и в отношении них оперативно («за часы») могут быть приняты меры защиты информации, нейтрализующие эти угрозы;

в) в информационной системе обеспечивается низкий уровень защищенности (Y1), если в ходе эксплуатации информационной системы появились дополнительные угрозы безопасности информации и в отношении них не могут быть с высокой оперативностью или оперативно приняты меры защиты информации, нейтрализующие эти угрозы.

В ходе эксплуатации системы в течение нескольких лет, возникали дополнительные угрозы безопасности информации, в отношении которых были приняты меры по их нейтрализации в течение нескольких часов.

Таким образом, можно сделать вывод, что информационная система имеет средний уровень исходной защищённости.

Возможность реализации j -ой угрозы безопасности информации (Y_j) в зависимости от уровня защищенности информационной системы ($Y_{1П}$) и потенциала нарушителя (Y_2) определяется как высокая, средняя или низкая в соответствии с таблицей 12.

Таблица 12 — Возможность реализации угрозы безопасности информации

Уровень защищённости	Высокий	Средний	Низкий
Потенциал нарушителя			
Базовый(низкий)	Низкая	Средняя	Высокая
Базовый повышенный(средний)	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

7.2 Оценка степени возможного ущерба от реализации угрозы безопасности информации

Для оценки степени возможного ущерба от реализации угрозы безопасности информации определяются возможный результат реализации угрозы безопасности информации в информационной системе, вид ущерба, к которому может привести реализация угрозы безопасности информации, степень последствий от реализации угрозы безопасности информации для каждого вида ущерба.

В качестве результата реализации угрозы безопасности информации рассматриваются непосредственное или опосредованное воздействие на конфиденциальность, целостность, доступность информации, содержащейся в информационной системе.

Результат реализации угрозы безопасности информации определяется воздействием угрозы на каждое свойство безопасности информации (конфиденциальность, целостность, доступность) в отдельности в соответствии

с таблицей 13. При обработке в информационной системе двух и более видов информации (служебная тайна, персональные данные, налоговая тайна, иные установленные законодательством Российской Федерации виды информации) воздействие на конфиденциальность, целостность, доступность определяется отдельно для каждого вида информации, содержащейся в информационной системе.

Таблица 13 - Результат реализации угрозы безопасности информации

Свойство безопасности информации	Результат реализации угрозы безопасности информации	
	Не оказывает воздействия	Оказывает воздействие
Конфиденциальность Хк	В результате реализации угрозы безопасности информации отсутствует возможность неправомерного доступа, копирования, предоставления или распространения информации	В результате реализации угрозы безопасности информации возможны неправомерный доступ, копирование, предоставление или распространение информации
Целостность Хц	В результате реализации угрозы безопасности информации отсутствует возможность уничтожения или модифицирования информации	В результате реализации угрозы безопасности информации возможно уничтожение или модифицирование информации
Доступность Хд	В результате реализации угрозы безопасности информации отсутствует возможность блокирования информации	В результате реализации угрозы безопасности информации возможно блокирование информации

Основные виды ущерба и возможные негативные последствия, к которым может привести нарушение конфиденциальности, целостности, доступности информации, приведены в таблице 14.

Таблица 14 — Вид ущерба и возможные негативные последствия

Вид ущерба	Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации
Экономический (финансовый)	<p>Снижение, как минимум, одного экономического показателя.</p> <p>Потеря (кража) финансовых средств.</p> <p>Недополучение ожидаемой (прогнозируемой) прибыли.</p> <p>Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.</p> <p>Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).</p>

Продолжение таблицы 14

Вид ущерба	Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации
Экономический (финансовый)	<p>Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.</p> <p>Потеря клиентов, поставщиков.</p> <p>Потеря конкурентного преимущества.</p> <p>Невозможность заключения договоров, соглашений.</p> <p>Другие прямые или косвенные финансовые потери</p>
Социальный	<p>Создание предпосылок для нанесения вреда здоровью граждан.</p> <p>Возможность нарушения функционирования объектов обеспечения жизнедеятельности граждан.</p> <p>Организация пикетов, забастовок, митингов и других акций.</p> <p>Увольнения.</p> <p>Увеличение количества жалоб в органы государственной власти или органы местного самоуправления.</p> <p>Появление негативных публикаций в общедоступных источниках.</p> <p>Невозможность (прерывание) предоставления социальных услуг (сервисов).</p> <p>Другие последствия, приводящие к нарастанию социальной напряженности в обществе</p>
Политический	<p>Создание предпосылок к обострению отношений в международных отношениях.</p> <p>Срыв двусторонних (многосторонних) контактов с зарубежными партнерами.</p> <p>Неспособность выполнения международных (двусторонних) договорных обязательств.</p> <p>Невозможность заключения международных (двусторонних) договоров, соглашений.</p> <p>Создание предпосылок к внутривнутриполитическому кризису.</p> <p>Нарушение выборного процесса.</p> <p>Другие последствия во внутривнутриполитической и внешнеполитической областях деятельности</p>
Репутационный	<p>Нарушение законодательных и подзаконных актов. Нарушение деловой репутации.</p> <p>Снижение престижа.</p> <p>Дискредитация работников.</p> <p>Утрата доверия.</p> <p>Неспособность выполнения договорных обязательств.</p> <p>Другие последствия, приводящие к нарушению репутации</p>
Ущерб в области обороны, безопасности и правопорядка	<p>Создание предпосылок к наступлению негативных последствий для обороны, безопасности и правопорядка.</p> <p>Нарушение общественного правопорядка.</p> <p>Неблагоприятное влияние на обеспечение общественного правопорядка.</p> <p>Возможность потери или снижения уровня контроля за общественным правопорядком.</p> <p>Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации.</p> <p>Другие последствия, приводящие к ущербу в области обороны, безопасности и правопорядка</p>

Продолжение таблицы 14

Вид ущерба	Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации
Ущерб субъекту персональных данных	Создание угрозы личной безопасности. Финансовые или иные материальные потери физического лица. Вторжение в частную жизнь. Создание угрозы здоровью. Моральный вред. Утрата репутации. Другие последствия, приводящие к нарушению прав субъекта персональных данных
Технологический	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Принятие неправильных решений. Простой информационной системы или сегмента информационной системы. Другие последствия, приводящие к нарушению технологии обработки информации

Степень возможного ущерба определяется экспертным методом в соответствии с таблицей 15.

Таблица 15 — Степень возможного ущерба

Степень ущерба	Характеристика степени ущерба
Высокая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
Средняя	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
Низкая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств

При обработке в информационной системе двух и более видов информации (служебная тайна, персональные данные, налоговая тайна и иные установленные законодательством Российской Федерации виды информации)

степень возможного ущерба определяется отдельно для каждого вида информации, обрабатываемой в информационной системе, применительно к каждому виду ущерба. Итоговая степень возможного ущерба устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации применительно к каждому виду ущерба.

7.3 Определение актуальности угрозы безопасности информации

Актуальной считается угроза, которая может быть реализована в ИС и представляет опасность для неё. Для определения актуальности конкретной угрозы безопасности ИС определяются:

- возможность реализации угрозы;
- опасность угрозы.

Решение об актуальности угрозы безопасности информации для информационной системы с заданными структурно-функциональными характеристиками и условиями функционирования принимается в соответствии с таблицей 16.

Таблица 16 — Финальная оценка актуальности угрозы

Вероятность (возможность) реализации угрозы	Степень возможного ущерба		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

Расчёт коэффициентов реализуемости для угроз из банка угроз ФСТЭК[9] для ИС, а также отнесение угроз к актуальным согласно правил, приведенных в таблице 16, приведено в таблице 17.

Таблица 17 — Расчёт коэффициентов реализуемости для каждой угрозы в ИС и определение актуальных угроз

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
1	Угроза автоматического распространения вредоносного кода в грид-системе	Угроза заключается в возможности внедрения и запуска вредоносного кода от имени доверенного процесса на любом из ресурсных центров грид-системы и его автоматического распространения на все узлы грид-системы. Данная угроза обусловлена слабостями технологии грид-вычислений – высоким уровнем автоматизации при малой администрируемости грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий легального пользователя грид-системы	С						Данная технология не применяется в ИС
2	Угроза агрегирования данных, передаваемых в грид-системе	Угроза заключается в возможности раскрытия нарушителем защищаемой информации путём выявления задействованных в её обработке узлов, сбора, анализа и обобщения данных, перехватываемых в сети передачи данных грид-системы. Данная угроза обусловлена слабостью технологии грид-вычислений – использованием незащищённых каналов сети Интернет как транспортной сети грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя: сил и средств, достаточных для компенсации чрезвычайной распределённости грид-заданий между узлами грид-системы; привилегий, достаточных для перехвата трафика сети передачи данных между элементами (узлами) грид-системы/	С						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
3	Угроза анализа криптографических алгоритмов и их реализации	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	С	ПДН	К	Социальный;	В	Актуальная	
						Репутационный;	В		
						Ущерб субъекту ПДН	В		
				СТ	К	Репутационный;	С		
						Социальный	С		
4	Угроза аппаратного сброса пароля BIOS	Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера	Н	ПДН	Ц	Технологический	Н	Неактуальная	
				СТ	Ц	Технологический	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
5	Угроза внедрения вредоносного кода в BIOS	Угроза заключается в возможности заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения BIOS/UEFI на версию, уже содержащую вредоносный код. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI и заменой чипсета BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера	В	ПДН	К	Ущерб субъекту ПДН	В	Актуальная	
					Ц	Технологический	С		
					Д	Репутационный	В		
				СТ	К	Социальный	С		
					Ц	Технологический	С		
					Д	Технологический	С		
6	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).	Н	ПДН	К	Ущерб субъекту ПДН	В	Актуальная	
					Ц	Технологический	Н		
					Д	Репутационный	С		
				СТ	К	Социальный	С		
					Ц	Репутационный	С		
					Д	Политический; Экономический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
6		Реализация данной угрозы возможна: в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников; при наличии у него привилегий установки программного обеспечения; в случае неизменных владельцем учетных данных IoT-устройства (заводских пароля и логина)							
7	Угроза воздействия на программы с высокими привилегиями	Угроза заключается в возможности повышения нарушителем своих привилегий в дискредитированной системе (получения привилегии дискредитированных программ) путём использования ошибок в программах и выполнения произвольного кода с их привилегиями. Данная угроза обусловлена слабостями механизма проверки входных данных и команд, а также мер по разграничению доступа. Реализация данной угрозы возможна при условиях: обладания дискредитируемой программой повышенными привилегиями в системе; осуществления дискредитируемой программой приёма входных данных от других программ или от пользователя; нарушитель имеет возможность осуществлять передачу данных к дискредитируемой программе	С	ПДН	К	Ущерб субъекту ПДН	С	Актуальная	
					Ц	Репутационный	С		
				СТ	К	Политический	С		
					Ц	Экономический	С		
8	Угроза восстановления аутентификационной информации	Угроза заключается в возможности подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе. Данная угроза обусловлена значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой, что определяет два следствия: время подбора в основном определяется не объёмом аутентификационной информации, а объёмом данных её хеш-кода; восстановленная аутентификационная информация может не совпадать	Н	ПДН	К	Ущерб субъекту ПДН	Н	Неактуальная	
				СТ	К	Репутационный	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
8		с исходной (при применении некоторых алгоритмов для нескольких наборов исходных данных могут быть получены одинаковые результаты – хеш-коды). Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную»							
9	Угроза восстановления предыдущей уязвимой версии BIOS	Угроза заключается в возможности осуществления вынужденного перехода на использование BIOS/UEFI, содержащей уязвимости. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. При использовании технологии обновления BIOS/UEFI возможно возникновение следующей ситуации (условия, характеризующие ситуацию указаны в хронологическом порядке): на компьютере установлена некоторая версия BIOS/UEFI, для которой на момент её работы не известны уязвимости; в силу некоторых обстоятельств BIOS/UEFI проходит процедуру обновления, сохраняя при этом предыдущую версию BIOS/UEFI на случай «отката» системы; публикуются данные о существовании уязвимостей в предыдущей версии BIOS/UEFI; происходит сбой в работе системы, в результате чего текущая (новая) версия BIOS/UEFI становится неработоспособной (например, нарушается её целостность); пользователь осуществляет штатную процедуру восстановления работоспособности системы – проводит «откат» системы к предыдущему работоспособному состоянию	Н	ПДН	К	Ущерб субъекту ПДН	Н	Неактуальная	
					Ц	Технологический	Н		
					Д	Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический	Н		
					Д	Технологический Репутационный	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
10	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 выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора	С	ПДН	К	Ущерб субъекту ПДН	В	Актуальная	
					Ц	Технологический	Н		
					Д	Технологический	Н		
				СТ	К	Социальный	С		
					Ц	Технологический	В		
					Д	Репутационный	С		
11	Угроза деавторизации санкционированного клиента беспроводной сети	Угроза заключается в возможности автоматического разрыва соединения беспроводной точки доступа с санкционированным клиентом беспроводной сети. Данная угроза обусловлена слабостью технологий сетевого взаимодействия по беспроводным каналам передачи данных – сведения о MAC-адресах беспроводных клиентов доступны всем участникам сетевого взаимодействия. Реализация данной угрозы возможна при условии подключения нарушителем к беспроводной сети устройства, MAC-адрес которого будет полностью совпадать с MAC-адресом дискредитируемого санкционированного клиента	Н	ПДН	Д	Репутационный	С	Актуальная	
				СТ	Д	Репутационный	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
12	Угроза деструктивного изменения конфигурации/среды окружения программ	Угроза заключается в возможности деструктивного программного воздействия на дискредитируемое приложение путём осуществления манипуляций с используемыми им конфигурационными файлами или библиотеками. Данная угроза обусловлена слабостями мер контроля целостности конфигурационных файлов или библиотек, используемых приложениями. Реализация данной угрозы возможна в случае наличия у нарушителя прав осуществления записи в файловые объекты, связанные с конфигурацией/средой окружения программы, или возможности перенаправления запросов дискредитируемой программы от защищённых файловых объектов к ложным	Н	ПДН	К	Ущерб субъекту ПДН	С	Актуальная	
					Ц	Технологический	С		
					Д	Социальный Репутационный	С		
				СТ	К	Репутационный	С		
					Ц	Технологический	С		
					Д	Репутационный	С		
13	Угроза деструктивного использования декларированного функционала BIOS	Угроза заключается в возможности неправомерного использования декларированного функционала BIOS/UEFI для нарушения целостности информации, хранимой на внешних носителях информации и в оперативном запоминающем устройстве компьютера. Данная угроза обусловлена уязвимостями программного обеспечения BIOS/UEFI, предназначенного для тестирования и обслуживания компьютера (средств проверки целостности памяти, программного обеспечения управления RAID-контроллером и т.п.). Реализации данной угрозы может способствовать возможность обновления некоторых BIOS/UEFI без прохождения аутентификации	Н	ПДН	Ц	Репутационный	Н	Неактуальная	
				СТ	Ц	Технологический	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
14	Угроза длительного удержания вычислительных ресурсов пользователями	Угроза заключается в возможности ограничения нарушителем доступа конечных пользователей к вычислительному ресурсу за счёт принудительного удержания его в загруженном состоянии путём осуществления им многократного выполнения определённых деструктивных действий или эксплуатации уязвимостей программ, распределяющих вычислительные ресурсы между задачами. Данная угроза обусловлена слабостями механизмов балансировки нагрузки и распределения вычислительных ресурсов. Реализация угрозы возможна в случае, если у нарушителя имеется возможность делать запросы, которые в совокупности требуют больше времени на выполнение, чем запросы пользователя	Н	ПДН	Д	Репутационный	С	Актуальная	
				СТ	Д	Технологический	С		
15	Угроза доступа к защищаемым файлам с использованием обходного пути	Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы. Реализация данной угрозы возможна при условиях: наличие у нарушителя прав доступа к некоторым объектам файловой системы; отсутствие проверки вводимых пользователем данных; наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с её помощью	Н	ПДН	К	Ущерб субъекту ПДН	С	Актуальная	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
16	Угроза доступа к локальным файлам сервера при помощи URL	Угроза заключается в возможности передачи нарушителем дискредитируемому браузеру запроса на доступ к файловой системе пользователя вместо URL-запроса. При этом браузер выполнит этот запрос с правами, которыми он был наделён при запуске, и передаст данные, полученные в результате выполнения этой операции, нарушителю. Данная угроза обусловлена слабостями механизма проверки вводимых пользователем запросов, который не делает различий между запросами на доступ к файловой системе и URL-запросами. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
				СТ	К	Социальный Репутационный	С		
17	Угроза доступа/перехвата/изменения HTTP cookies	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации (учётным записям пользователей, сертификатам и т.п.), содержащейся в cookies-файлах, во время их хранения или передачи, в режиме чтения (раскрытие конфиденциальности) или записи (внесение изменений для реализации угрозы подмены доверенного пользователя). Данная угроза обусловлена слабостями мер защиты cookies-файлов: отсутствием проверки вводимых данных со стороны сетевой службы, использующей cookies-файлы, а также отсутствием шифрования при передаче cookies-файлов. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к cookies-файлам и отсутствии проверки целостности их значений со стороны дискредитируемого приложения	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Д	Репутационный	С		
				СТ	К	Репутационный	С		
					Д	Технологический	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
18	Угроза загрузки нештатной операционной системы	Угроза заключается в возможности подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии доступности нарушителю следующего параметра настройки BIOS/UEFI – указания источника загрузки операционной системы	Н	ПДН	К	Ущерб субъекту ПДН	Н	Неактуальная	
					Ц	Технологический	Н		
					Д	Репутационный	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический	Н		
					Д	Технологический	Н		
19	Угроза заражения DNS-кеша	Угроза заключается в возможности перенаправления нарушителем сетевого трафика через собственный сетевой узел путём опосредованного изменения таблиц соответствия IP- и доменных имён, хранимых в DNS-сервере, за счёт генерации лавины возможных ответов на запрос DNS-сервера легальному пользователю или за счёт эксплуатации уязвимостей DNS-сервера. Данная угроза обусловлена слабостями механизмов проверки подлинности субъектов сетевого взаимодействия, а также уязвимостями DNS-сервера, позволяющими напрямую заменить DNS-кеш DNS-сервера. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий, достаточных для отправки сетевых запросов к DNS-серверу	Н	ПДН	К	Ущерб субъекту ПДН	Н	Неактуальная	
				СТ	К	Репутационный	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
20	Угроза злоупотребления возможностями, предоставляемыми потребителям облачных услуг	Угроза заключается в возможности осуществления потребителем облачных услуг (нарушителем) рассылки спама, несанкционированного доступа к виртуальным машинам других потребителей облачных услуг или осуществления других деструктивных программных воздействий на различные системы с помощью арендованных ресурсов облачного сервера. Данная угроза обусловлена тем, что потребитель облачных услуг может устанавливать собственное программное обеспечение на облачный сервер. Реализация данной угрозы возможна путём установки и запуска потребителем облачных услуг вредоносного программного обеспечения на облачный сервер. Успешная реализация данной угрозы потребителем облачных услуг оказывает негативное влияние на репутацию поставщика облачных услуг	Н	ПДН	К	Репутационный			Данная технология не применяется в ИС
					Ц	Репутационный			
					Д	Репутационный			
				СТ	К	Репутационный			
					Ц	Технологический			
					Д	Технологический			
21	Угроза злоупотребления доверием потребителем 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)	Н	ПДН	К	Репутационный			Данная технология не применяется в ИС
					Ц	Репутационный			
				СТ	К	Репутационный			
					Ц	Технологический			

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
22	Угроза избыточного выделения оперативной памяти	Угроза заключается в возможности выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти, доступных в системе для выделения в ответ на запросы программ легальных пользователей. Данная угроза обусловлена наличием слабостей механизма контроля выделения оперативной памяти различным программам. Реализация данной угрозы возможна при условии нахождения вредоносного программного обеспечения в системе в активном состоянии	Н	ПДН	Д	Технологический	Н	Актуальная	
				СТ	Д	Технологический	С		
23	Угроза изменения компонентов системы	Угроза заключается в возможности получения нарушителем доступа к сети Интернет (при его отсутствии в системе), к хранимым на личных мобильных устройствах 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	Н	ПДН	Ц	Технологический	С	Актуальная	
					Д	Социальный	Н		
				СТ	Ц	Технологический	С		
					Д	Технологический	Н		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
24	Угроза изменени я режимов работы аппаратн ых элементов компьюте ра	Угроза заключается в возможности изменения нарушителем режимов работы аппаратных элементов компьютера путём несанкционированного переконфигурирования BIOS/UEFI, что позволяет: за счёт изменения частоты системной шины, режима передачи данных по каналам связи и т.п. повлиять на общую производительность компьютера или вызвать сбои в его работе; за счёт понижения входного напряжения, отключения систем охлаждения временно обеспечить неработоспособность компьютера; за счёт задания недопустимых параметров работы устройств (порогового значения отключения устройства при перегреве, входного напряжения и т.п.) привести к физическому выходу из строя отдельных аппаратных элементов компьютера. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение соответствующих параметров настройки	В	ПДН	Ц	Технологический	В	Акту альна я	
					Д	Технологический	С		
				СТ	Ц	Технологический	В		
					Д	Технологический	С		
25	Угроза изменени я системны х и глобальны х переменн ых	Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путём изменения используемых дискредитируемыми программами единых системных и глобальных переменных. Данная угроза обусловлена слабостями механизма контроля доступа к разделяемой памяти, а также уязвимостями программных модулей приложений, реализующих контроль целостности внешних переменных. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к системным и глобальным переменным и отсутствии проверки целостности их значений со стороны дискредитируемого приложения	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Социальный Технологический	С		
					Д	Технологический	С		
				СТ	К	Социальный	С		
					Ц	Технологический	В		
					Д	Технологический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
26	Угроза искажения XML-схемы	Угроза заключается в возможности изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером. Данная угроза обусловлена слабостями мер обеспечения целостности передаваемых при клиент-серверном взаимодействии данных, а также слабостями 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	С	ПДН	Ц	Репутационный Социальный Технологический	В	Акту альна я	
					Д	Репутационный Социальный	С		
				СТ	Ц	Технологический	В		
					Д	Технологический	С		
27	Угроза искажения и выводимой на периферийн ые устройства информации	Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок						Неакту альна я	Не применима к рассматрив аемой системе

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
28	Угроза использования альтернативных путей доступа к ресурсам	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса). Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации, слабостями фильтрации входных данных. Реализация данной угрозы возможна при условии наличия у нарушителя: возможности ввода произвольных данных в адресную строку; сведений о пути к защищаемому ресурсу; возможности изменения интерфейса ввода входных данных	Н	ПДН	К	Репутационный Социальный	С	Актуальная	
				СТ	К	Социальный Репутационный	С		
29	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Угроза заключается в возможности существенного снижения производительности вычислительного поля суперкомпьютера и эффективности выполнения на нём текущих параллельных вычислений из-за потребления вычислительных ресурсов суперкомпьютера «паразитными» процессами («процессами-потомками» предыдущих заданий или процессами, запущенными вредоносным программным обеспечением). Данная угроза обусловлена слабостями мер очистки памяти от «процессов-потомков» завершённых заданий, а также процессов, запущенных вредоносным программным обеспечением. Реализация данной угрозы возможна при условии некорректного завершения выполненных задач или наличия вредоносных процессов в памяти суперкомпьютера в активном состоянии						Неактуальная	Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	<p>Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты.</p> <p>Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset).</p> <p>Реализация данной угрозы возможна при одном из следующих условий: наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты; успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты</p>	Внутренний нарушитель с низким потенциалом	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный	Н		
				СТ	К	Ущерб субъекту ПДН Социальный	Н		
					Ц	Технологический	С		
					Д	Технологический	С		
			Внешний нарушитель со средним потенциалом	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С		
					Ц	Репутационный	С		
					Д	Репутационный	Н		
				СТ	К	Ущерб субъекту ПДН Социальный	Н		
					Ц	Технологический	С		
					Д	Технологический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
31	Угроза использования механизмов авторизации для повышения привилегий	Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки. Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе	Н	ПДН	К	Репутационный Социальный Ущерб субъекту ПДН	С	Актуальная	
				СТ	К	Репутационный Ущерб субъекту ПДН	Н		
32	Угроза использования поддельных цифровых подписей BIOS	Угроза заключается в возможности установки уязвимой версии обновления BIOS/UEFI или версии, содержащей вредоносное программное обеспечение, но имеющей цифровую подпись. Данная угроза обусловлена слабостями мер по контролю за благонадёжностью центров выдачи цифровых подписей. Реализация данной угрозы возможна при условии выдачи неблагонадёжным центром сертификации цифровой подписи на версию обновления BIOS/UEFI, содержащую уязвимости, или на версию, содержащую вредоносное программное обеспечение (т.е. при осуществлении таким центром подлога), а также подмены нарушителем доверенного источника обновлений	С	ПДН	Ц	Репутационный Социальный	С	Актуальная	
				СТ	Ц	Технологический Экономический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
33	Угроза использован ия 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	С	ПДН	Ц	Репутационный Социальный Технологический	С	Акту альна я	
					Д	Репутационный Технологический	Н		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический	Н		
34	Угроза использован ия слабостей протоколов сетевого/лок ального обмена данными	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов. Данная угроза обусловлена слабостями самих протоколов (заложенных в них алгоритмов), ошибками, допущенными в ходе реализации протоколов, или уязвимостями, внедряемыми автоматизированными средствами проектирования/разработки. Реализация данной угрозы возможна в случае наличия слабостей в протоколах сетевого/локального обмена данными	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы 17

№ уgroзы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
35	Угроза использования слабых криптографических алгоритмов BIOS	Угроза заключается в сложности проверки реальных параметров работы и алгоритмов, реализованных в криптографических средствах BIOS/UEFI. При этом доверие к криптографической защите будет ограничено доверием к производителю BIOS. Данная угроза обусловлена сложностью использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI. Возможность реализации данной угрозы снижает достоверность оценки реального уровня защищённости системы	В	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный	С		
				СТ	К	Ущерб субъекту ПДН Социальный	С		
					Ц	Технологический	В		
					Д	Технологический	С		
36	Угроза исследования механизмов работы программы	Угроза заключается в возможности проведения нарушителем обратного инжиниринга кода программы и дальнейшего исследования его структуры, функционала и состава в интересах определения алгоритма работы программы и поиска в ней уязвимостей. Данная угроза обусловлена слабостями механизма защиты кода программы от исследования. Реализация данной угрозы возможна в случаях: наличия у нарушителя доступа к исходным файлам программы; наличия у нарушителя доступа к дистрибутиву программы и отсутствия механизма защиты кода программы от исследования	С	ПДН				Неактуальная	Не применима к рассматриваемой системе
				СТ					

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
37	Угроза исследования приложения через отчёты об ошибках	Угроза заключается в возможности исследования нарушителем алгоритма работы дискредитируемого приложения и его предполагаемой структуры путём анализа генерируемых этим приложением отчётов об ошибках. Данная угроза обусловлена размещением защищаемой информации (или информации, обобщение которой может раскрыть защищаемые сведения о системе) в генерируемых отчётах об ошибках. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Ущерб субъекту ПДН Репутационный	С		
38	Угроза истощения вычислительных ресурсов хранилища больших данных	Угроза заключается в возможности временного возникновения состояния типа «отказ в обслуживании» у хранилища больших данных. Данная угроза обусловлена постоянным трудно контролируемым заполнением занятого дискового пространства за счёт данных, непрерывно поступающих из различных информационных источников, и слабостями технологий доступа и хранения информации в хранилищах больших данных. Реализация данной угрозы возможна при условии мгновенного (текущего) превышения скорости передачи данных над скоростью их сохранения (в силу недостаточности пропускной способности канала связи или скорости выделения свободного пространства и сохранения на него поступающих данных) или при условии временного отсутствия свободного места в хранилище (в силу некорректного управления хранилищем или в результате осуществления нарушителем деструктивного программного воздействия на механизм контроля за заполнением хранилища путём изменения параметров или логики его работы)	Н	ПДН				Не актуальная	Данная технология не применяется в ИС
				СТ					

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Угроза заключается в возможности нарушения (невозможности осуществления) процедуры обновления BIOS/UEFI при исчерпании запаса необходимых для её проведения ключей. Данная угроза обусловлена ограниченностью набора ключей, необходимых для обновления BIOS/UEFI. Реализация данной угрозы возможна путём эксплуатации уязвимостей средств обновления набора ключей, или путём использования нарушителем программных средств перебора ключей	С	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
				СТ	Ц	Репутационный Технологический	С		
40	Угроза конфликта юрисдикций различных стран	Угроза заключается в возможности отказа в трансграничной передаче защищаемой информации в рамках оказания облачных услуг в соответствии с требованиями локального законодательства стран, резиденты которых участвуют в оказании облачных услуг. Данная угроза обусловлена тем, что в зависимости от особенностей законодательства различных стран, резиденты которых участвуют в оказании облачных услуг, при обеспечении информационной безопасности могут использоваться правовые меры различных юрисдикций. 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	Н	ПДН				Не актуа льная	Не применима к рассматрив аемой системе
				СТ					

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
41	Угроза межсайтового скриптинга	Угроза заключается в возможности внедрения нарушителем участков вредоносного кода на сайт дискредитируемой системы таким образом, что он будет выполнен на рабочей станции просматривающего этот сайт пользователя. Данная угроза обусловлена слабостями механизма проверки безопасности при обработке запросов и данных, поступающих от веб-сайта. Реализация угрозы возможна в случае, если клиентское программное обеспечение поддерживает выполнение сценариев, а нарушитель имеет возможность отправки запросов и данных в дискредитируемую систему	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Технологический Социальный	В	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Технологический Социальный	С		
					Ц	Технологический	В		
					Д	Технологический	С		
42	Угроза межсайтовой подделки запроса	Угроза заключается в возможности отправки нарушителем дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс, при переходе на который автоматически будут выполнены неправомерные вредоносные действия от имени дискредитированного пользователя. Данная угроза обусловлена уязвимостями браузеров, которые позволяют выполнять действия без подтверждения или аутентификации со стороны дискредитируемого пользователя. Реализация угрозы возможна в случае, если дискредитируемый пользователь сохраняет аутентификационную информацию с помощью браузера	С	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический	С		
					Д	Технологический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обраба тываем ой инфор мации	Нарушаемы е свойства безопаснос ти информаци и	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
43	Угроза нарушения доступности облачного сервера	Угроза заключается в возможности прекращения оказания облачных услуг всем потребителям (или группе потребителей) из-за нарушения доступности для них облачной инфраструктуры. Данная угроза обусловлена тем, что обеспечение доступности не является специфичным требованием безопасности информации для облачных технологий, и, кроме того, облачные системы реализованы в соответствии с сервис-ориентированным подходом. Реализация данной угрозы возможна при переходе одного или нескольких облачных серверов в состояние «отказ в обслуживании». Более того, способность динамически изменять объём предоставляемых потребителям облачных услуг может быть использована нарушителем для реализации угрозы. При этом успешно реализованная угроза в отношении всего лишь одного облачного сервиса позволит нарушить доступность всей облачной системы	Н	ПДН	Д			Не актуальная	Данная технология не применяется в ИС
				СТ	Д				
44	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Угроза заключается в возможности нарушения безопасности пользовательских данных программ, функционирующих внутри виртуальной машины, вредоносным программным обеспечением, функционирующим вне виртуальной машины. Данная угроза обусловлена наличием уязвимостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри виртуальной машины, от несанкционированного доступа со стороны вредоносного программного обеспечения, функционирующего вне виртуальной машины. Реализация данной угрозы возможна при условии успешного преодоления вредоносным программным кодом границ виртуальной машины не только за счёт эксплуатации уязвимостей гипервизора, но и путём осуществления такого воздействия с более низких (по отношению к гипервизору) уровней функционирования системы	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический	С		
					Д	Технологический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
45	Угроза нарушения изоляции среды исполнения BIOS	Угроза заключается в возможности изменения параметров и (или) логики работы программного обеспечения BIOS/UEFI путём программного воздействия из операционной системы компьютера или путём несанкционированного доступа к каналу сетевого взаимодействия серверного сервис-процессора. Данная угроза обусловлена слабостями технологий разграничения доступа к BIOS/UEFI, его функциям администрирования и обновления, со стороны операционной системы или каналов связи. Реализация данной угрозы возможна: со стороны операционной системы – при условии наличия BIOS/UEFI функционала обновления и (или) управления программным обеспечением BIOS/UEFI из операционной системы; со стороны сети – при условии наличия у дискредитируемого серверного сервис-процессора достаточных привилегий для управления всей системой, включая модификацию BIOS/UEFI серверов системы, и дискредитируемого сервера	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный	Н		
					Д	Репутационный	Н		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
46	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия. Данная угроза обусловлена наличием множества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между её уровнями. Реализация данной угрозы возможна в случае возникновения ошибок при проведении аутентификации субъектов виртуального информационного взаимодействия	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Д	Репутационный	Н		
				СТ	К	Репутационный Социальный	Н		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
47	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Угроза заключается в возможности значительного снижения производительности грид-системы, вплоть до временного нарушения её работоспособности при появлении нетипичной сетевой нагрузки (в т.ч. вызванной распределённой DoS-атакой, активностью других пользователей в сети и др.). Данная угроза обусловлена слабостью технологий грид-вычислений – производительность грид-системы имеет сильную зависимость от загруженности каналов связи, что является следствием максимальной территориальной распределённости вычислительного модуля грид-системы среди всех типов информационных систем. Реализация данной угрозы возможна при условии недостаточного контроля за состоянием отдельных узлов грид-системы со стороны диспетчера задач грид-системы	С					Не актуальная	Данная технология не применяется в ИС
48	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через неё на другие системы путём осуществления несанкционированного доступа к образам виртуальных машин. Данная угроза обусловлена слабостями мер разграничения доступа к образам виртуальных машин, реализованных в программном обеспечении виртуализации. Реализация данной угрозы может привести: к нарушению конфиденциальности защищаемой информации, обрабатываемой с помощью виртуальных машин, созданных на основе несанкционированно изменённых образов; к нарушению целостности программ, установленных на виртуальных машинах; к нарушению доступности ресурсов виртуальных машин.	С	ПДН	К	Ущерб субъекту ПДН Репутационный\Социальный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
49	Угроза нарушения целостности данных кеша	Угроза заключается в возможности размещения нарушителем в кеше приложения (например, браузера) или службы (например, DNS или ARP) некорректных (потенциально опасных) данных таким образом, что до обновления кеша дискредитируемое приложение (или служба) будет считать эти данные корректными. Данная угроза обусловлена слабостями в механизме контроля целостности данных в кеше. Реализация данной угрозы возможна в условиях осуществления нарушителем успешного несанкционированного доступа к данным кеша и отсутствии проверки целостности данных в кеше со стороны дискредитируемого приложения (или службы)	Н	ПДН	Ц	Репутационный	Н	Не актуальная	
					Д	Репутационный	Н		
				СТ	Ц	Технологический Экономический	Н		
					Д	Технологический	Н		
50	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Угроза заключается в возможности искажения информации, сохраняемой в хранилище больших данных, или отказа в проведении сохранения при передаче в него данных в некоторых форматах. Данная угроза обусловлена слабостями технологий определения формата входных данных на основе дополнительной служебной информации (заголовки файлов и сетевых пакетов, расширения файлов и т.п.), а также технологий адаптивного выбора и применения методов обработки мультимедийной 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 содержанию, или в хранилище больших данных не реализованы методы обработки данных получаемого формата	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
51	Угроза невозможно сти восстано вления сессии работы на ПЭВМ при выводе из промежуточ ных 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.)	Н	ПДН	Ц	Репутационный	Н	Акту альна я	
					Д	Репутационный	Н		
					Ц	Репутационный Экономический Технологический	С		
					Д	Репутационный Экономический Технологический	Н		
52	Угроза невозможно сти миграции образов виртуальных машин из-за несовмести мости аппаратного и программно го обеспечения	Угроза заключается в возможности возникновения у потребителя облачных услуг непреодолимых сложностей для смены поставщика облачных услуг из-за технических сложностей в реализации процедуры миграции образов виртуальных машин из облачной системы одного поставщика облачных услуг в систему другого. Данная угроза обусловлена тем, что каждый поставщик облачных услуг использует для реализации своей деятельности аппаратное и программное обеспечение различных производителей, часть которого может использовать специфические (для данного производителя) инструкции, протоколы, методы, схемы коммутации и другие особенности реализации своего функционала. Реализация данной угрозы возможна в случае несовместимости стандартных программных интерфейсов обмена данными (API) для реализации процедуры миграции образов виртуальных машин между различными поставщиками облачных услуг в одном или обоих направлениях.	Н						Данная технология не применяетс я в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
53	Угроза невозможности управления правами пользователей BIOS	Угроза заключается в возможности неправомерного использования пользователями декларированного функционала BIOS/UEFI, ориентированного на администраторов. Данная угроза обусловлена слабостями технологий разграничения доступа (распределения прав) к функционалу BIOS/UEFI между различными пользователями и администраторами. Реализация данной угрозы возможна при условии физического доступа к терминалу и, при необходимости, к системному блоку компьютера	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		
54	Угроза недобросовестного исполнения обязательств поставщика облачных услуг	Угроза заключается в возможности раскрытия или повреждения целостности поставщиком облачных услуг защищаемой информации потребителей облачных услуг, невыполнения требований к уровню качества (уровню доступности) предоставляемых потребителям облачных услуг доступа к их программам или иммигрированным в облако информационным системам. Данная угроза обусловлена невозможностью непосредственного контроля над действиями сотрудников поставщика облачных услуг со стороны их потребителей. Реализация данной угрозы возможна в случаях халатности со стороны сотрудников поставщика облачных услуг, недостаточности должностных и иных инструкций данных сотрудников, недостаточности мер по менеджменту и обеспечению безопасности облачных услуг и т.д.	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угроз	Обоснование
55	Угроза незащищённого администрирования облачных услуг	<p>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.</p> <p>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.</p> <p>Реализация данной угрозы возможна в случае получения нарушителем аутентификационной информации (при их вводе в общественных местах) легальных пользователей, или эксплуатации уязвимостей в средствах удалённого администрирования</p>	Н						Данная технология не применяется в ИС
56	Угроза некачественного переноса инфраструктуры в облако	<p>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.</p> <p>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).</p> <p>Реализация данной угрозы возможна в случае несовместимости программных и сетевых интерфейсов или несоответствий политик безопасности при осуществлении переноса информационной системы в облако</p>	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
57	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Угроза заключается в сложности контроля за всеми автоматически создаваемыми копиями информации в хранилище больших данных из-за временной несогласованности данных операций. Данная угроза обусловлена осуществлением дублирования (дву- или многократного) данных на различных вычислительных узлах, входящих в состав хранилища больших данных, с целью повышения скорости доступа к этим данным при большом количестве запросов чтения/записи. При этом данная операция является внутренней функцией и «непрозрачна» для конечных пользователей и администраторов хранилища больших данных. Реализация данной угрозы возможна при условии недостаточности мер по контролю за автоматически создаваемыми копиями информации, применяемых в хранилище больших данных	Н						Данная технология не применяется в ИС
58	Угроза неконтролируемого роста числа виртуальных машин	Угроза заключается в возможности ограничения или нарушения доступности виртуальных ресурсов для конечных потребителей облачных услуг путём случайного или несанкционированного преднамеренного создания нарушителем множества виртуальных машин. Данная угроза обусловлена ограниченностью объёма дискового пространства, выделенного под виртуальную инфраструктуру, и слабостями технологий контроля процесса создания виртуальных машин. Реализация данной угрозы возможна при условии наличия у нарушителя прав на создание виртуальных машин в облачной инфраструктуре	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
59	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	<p>Угроза заключается в возможности отказа легальным пользователям в выделении компьютерных ресурсов после осуществления нарушителем неправомерного резервирования всех свободных компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти).</p> <p>Данная угроза обусловлена уязвимостями программного обеспечения уровня управления виртуальной инфраструктурой, реализующего функцию распределения компьютерных ресурсов между пользователями.</p> <p>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</p>	Н	ПДН	Д	Репутационный Технологический	С	Актуальна	
				СТ	Д	Технологический	С		
60	Угроза неконтролируемого уничтожения информации хранилищем больших данных	<p>Угроза заключается в возможности удаления из хранилища некоторых обрабатываемых данных без уведомления конечного пользователя или администратора.</p> <p>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.).</p> <p>Реализация данной угрозы возможна при условии недостаточности реализованных в хранилище больших данных мер по контролю за автоматическим удалением данных</p>	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
61	Угроза некорректного задания структуры данных транзакции	Угроза заключается в возможности совершения нарушителем (клиентом базы данных) подлога путём прерывания транзакции или подмены идентификатора транзакции. В первом случае происходит неполное выполнение транзакции, а во втором – пользователь форсированно завершает транзакцию, изменяя её ID, и сообщая о том, что транзакция не была проведена, тем самым провоцируя повторное проведение транзакции. Данная угроза обусловлена слабостями механизма контроля непрерывности транзакций и целостности данных, передаваемых в ходе транзакции между базой данных и её клиентом	С	ПДН	Ц	Репутационный Технологический	С	Актуальная	
					Д	Технологический	С		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический	С		
62	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Угроза заключается в возможности перенаправления или копирования обрабатываемых браузером данных через прозрачный прокси-сервер, подключённый к 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Неактуальная	
				СТ	К	Репутационный	Н		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
63	Угроза некорректно го использован ия функционал а программно го и аппаратного обеспечения	Угроза заключается в возможности использования декларированных возможностей программных и аппаратных средств определённым (нестандартным, некорректным) способом с целью деструктивного воздействия на информационную систему и обрабатываемую ею информацию. Данная угроза связана со слабостями механизма обработки данных и команд, вводимых пользователями. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к программным и аппаратным средствам	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		
64	Угроза некорректно й реализации политики лицензирова ния в облаке	Угроза заключается в возможности отказа потребителям облачных услуг в удалённом доступе к арендуемому программному обеспечению (т.е. происходит потеря доступности облачной услуги SaaS) по вине поставщика облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками лицензирования использования программного обеспечения различных производителей в облаке. Реализация данной угрозы возможна при условии, что политика лицензирования использования программного обеспечения основана на ограничении количества его установок или числа его пользователей, а созданные виртуальные машины с лицензируемым программным обеспечением использованы много раз	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
65	Угроза неопределённости в распределении ответственности между ролями в облаке	Угроза заключается в возможности возникновения существенных разногласий между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей в части обеспечения информационной безопасности. 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)	Н						Данная технология не применяется в ИС
66	Угроза неопределённости ответственности за обеспечение безопасности и облака	Угроза заключается в возможности невыполнения ряда мер по защите информации как поставщиком облачных услуг, так и их потребителем. Данная угроза обусловлена отсутствием чёткого разделения ответственности в части обеспечения безопасности информации между потребителем и поставщиком облачных услуг. Реализация данной угрозы возможна при условии недостаточности документального разделения сфер ответственности между сторонами участвующими в оказании облачных услуг, а также отсутствия документального определения ответственности за несоблюдение требований безопасности	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
67	Угроза неправомерного ознакомления с защищаемой информацией	Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный	Н		
68	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API). 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	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
69	Угроза неправомерн ых 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический	Н		
70	Угроза непрерывно й модернизаци и облачной инфраструкт уры	Угроза заключается в возможности занесения в облачную систему уязвимостей и слабостей вместе с добавлением нового программного или аппаратного обеспечения. При этом система, рассматриваемая как защищённая на этапе ввода её в эксплуатацию, уже не может считаться таковой после её модернизации. Данная угроза обусловлена тем, что, во-первых, поставщики облачных услуг предоставляют возможность осуществления потребителем облачных услуг выбора и (или) изменения первоначального состава программного обеспечения облачной инфраструктуры в процессе оказания таких услуг, а, во-вторых, при интенсивном подключении новых потребителей модернизация облачной инфраструктуры может проходить несколько раз в год. Реализация данной угрозы возможна в случае, если срок до следующей модернизации не превышает срока проведения оценки соответствия системы требованиям безопасности в условиях отсутствия системы менеджмента облачных услуг и обеспечения их безопасности (системы облачного менеджмента)	С						Данная технология не применяетс я в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
71	Угроза несанкционированного восстановления удалённой защищаемой информации	<p>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.</p> <p>Данная угроза обусловлена слабостями механизма удаления информации с машинных носителей – информация, удалённая с машинного носителя, в большинстве случаев может быть восстановлена.</p> <p>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).</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный	С		
72	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	<p>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.</p> <p>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.</p> <p>Реализация данной угрозы возможна в одном из следующих условий: выключенном механизме защиты BIOS/UEFI от записи; успешной эксплуатации нарушителем уязвимости механизма обновления BIOS/UEFI, приводящей к переполнению буфера</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы 17

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путём эксплуатации уязвимостей программного и (или) микропрограммного обеспечения указанного оборудования. Данная угроза обусловлена ограниченностью функциональных возможностей (наличием слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры, наличием у данного оборудования фиксированного сетевого адреса. Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный	В		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		
74	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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
75	Угроза несанкционированного доступа к виртуальным каналам передачи	Угроза заключается в возможности осуществления нарушителем несанкционированного перехвата трафика сетевых узлов, недоступных с помощью сетевых технологий, отличных от сетевых технологий виртуализации, путём некорректного использования таких технологий. Данная угроза обусловлена слабостями мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных). Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Актуальная	
				СТ	К	Репутационный	С		
76	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор. 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. 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	С	ПДН	Д	Репутационный Технологический	С	Актуальная	
				СТ	Д	Технологический	С		

Продолжение таблицы 17

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
77	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	<p>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.</p> <p>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.</p> <p>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</p>	С	ПДН	Ц	Репутационный Технологический	Н	Актуальна	
					Д	Технологический	Н		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический	Н		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информа ции	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
78	Угроза несанкцион ированного доступа к защищаемы м виртуальны м машинам из виртуальной и (или) физической сети	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации. Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		
79	Угроза несанкцион ированного доступа к защищаемы м виртуальны м 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
80	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Угроза заключается в возможности удалённого осуществления нарушителем несанкционированного доступа к виртуальным устройствам из виртуальной и (или) физической сети с помощью различных сетевых технологий, используемых для осуществления обмена данными в системе, построенной с использованием технологий виртуализации. Данная угроза обусловлена наличием слабостей в сетевых программных интерфейсах гипервизоров, предназначенных для удалённого управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий достаточных для осуществления обмена данными в системе, построенной с использованием технологий виртуализации	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альная я	
					Ц	Репутационный Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		
81	Угроза несанкционированного доступа к сегментам вычислительного поля	Угроза заключается в возможности осуществления несанкционированного доступа нарушителя к исходным данным, промежуточным и окончательным результатам расчётов других пользователей суперкомпьютера, а также случайное или преднамеренное деструктивное воздействие процессов решения одних задач на процессы и результаты решения других вычислительных задач. Данная угроза обусловлена слабостями механизма разграничения доступа субъектов к сегментам вычислительных полей суперкомпьютера. Реализация данной угрозы возможна при выполнении задач различных пользователей суперкомпьютера на одном вычислительном поле суперкомпьютера	С	ПДН					Данная технология не применяется в ИС
				СТ					

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
82	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	<p>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.</p> <p>Данная угроза обусловлена наличием уязвимостей в клиенте грид-системы (клиентского программного обеспечения, устанавливаемого в узлах грид-системы), эксплуатация которых позволяет нарушителю осуществлять операции чтения и записи в объектах локальной файловой системы компьютера, отправку сигналов программным процессам (включая сигналы прекращения работы), операции чтения и записи в память программных процессов, соответствующих связующему программному обеспечению и грид-заданиям, открытия сетевых соединений в локальных и внешних узлах грид-системы.</p> <p>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)</p>	С						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
83	Угроза несанкционированного доступа к системе по беспроводным каналам	Угроза заключается в возможности получения нарушителем доступа к ресурсам всей дискредитируемой информационной системы через используемые в её составе беспроводные каналы передачи данных. Данная угроза обусловлена слабостями протоколов идентификации/аутентификации (таких как WEP, WPA и WPA2, 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 приёма сигналов дискредитируемой беспроводной сети	Н						Данная технология не применяется в ИС
84	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.	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
				СТ	К	Репутационный	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
85	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	<p>Угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски (являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путём логического объединения нескольких виртуальных устройств хранения данных).</p> <p>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.</p> <p>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.)</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Технологический Социальный	С		
					Д	Технологический Социальный	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
86	Угроза несанкционированного изменения аутентификационной информации	Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств. Данная угроза обусловлена наличием слабостей мер разграничения доступа к информации аутентификации. Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учётной записью дискредитированного пользователя	Н	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
					Д	Репутационный Технологический	С		
				СТ	Ц	Репутационный Технологический Экономический	С		
					Д	Репутационный Технологический	С		
88	Угроза несанкционированного копирования защищаемой информации	Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне. Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
87	Угроза несанкционированного использования привилегированных функций BIOS	Угроза заключается в возможности использования нарушителем потенциально опасных возможностей BIOS/UEFI. Данная угроза обусловлена наличием в BIOS/UEFI потенциально опасного функционала	Внутренний нарушитель с низким потенциалом	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
			Внешний нарушитель с высоким потенциалом	ПДН	К	Ущерб субъекту ПДН Репутационный	В		
					Ц	Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
89	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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Актуальная	
					Ц	Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
90	Угроза несанкционированного создания учётной записи пользователя	Угроза заключается в возможности создания нарушителем в системе дополнительной учётной записи пользователя и её дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учётной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации. Реализация данной угрозы возможна в случае наличия и прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
91	Угроза несанкционированного удаления защищаемой информации	Угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации путём осуществления деструктивного программного или физического воздействия на машинный носитель информации. Данная угроза обусловлена недостаточностью мер по обеспечению доступности защищаемой информации в системе, а равно и наличием уязвимостей в программном обеспечении, реализующим данные меры. Реализация данной угрозы возможна в случае получения нарушителем системных прав на стирание данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия	Н	ПДН	Д	Репутационный Технологический	С	Актуальная	
				СТ	Д	Технологический Экономический	С		
92	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Угроза заключается в возможности получения нарушителем привилегий управления системой путём использования удалённого внеполосного (по независимому вспомогательному каналу ТСР/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)	В	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Технологический Репутационный	С		
					Д	Технологический Репутационный	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
93	Угроза несанкционированного управления буфером	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся там информацией или осуществления деструктивного программного воздействия на систему (например, переполнение буфера для выполнения произвольного вредоносного кода). Данная угроза обусловлена слабостями в механизме разграничения доступа к буферу обмена, а также слабостями в механизмах проверки вводимых данных. Реализация данной угрозы возможна в случае осуществления нарушителем успешного несанкционированного доступа к сегменту оперативной памяти дискредитируемого объекта, в котором расположен буфер обмена	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Неактуальная	
					Ц	Технологический	Н		
					Д	Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	Н		
					Д	Технологический Экономический	Н		
95	Угроза несанкционированного управления указателями	Угроза заключается в возможности выполнения нарушителем произвольного вредоносного кода от имени дискредитируемого приложения или приведения дискредитируемого приложения в состояние «отказ в обслуживании» путём изменения указателей на ячейки памяти, содержащие определённые данные, используемые дискредитируемым приложением. Данная угроза связана с уязвимостями в средствах разграничения доступа к памяти и контроля целостности содержимого ячеек памяти. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение указателей, используемых дискредитируемым приложением	С	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Актуальная	
					Ц	Технологический Репутационный	Н		
					Д	Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	Н		
					Д	Технологический Экономический	Н		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
94	Угроза несанкционированного управления синхронизацией и состоянием	<p>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.).</p> <p>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.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя возможности:</p> <ul style="list-style-type: none"> 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) 	С	ПДН	Ц	Репутационный Технологический	В	Акту альна я	
					Д	Репутационный Технологический	В		
				СТ	Ц	Репутационный Технологический Экономический	В		
					Д	Репутационный Технологический	В		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
96	Угроза несогласованности политик безопасности и элементов облачной инфраструктуры	Угроза заключается в возможности осуществления нарушителем деструктивных программных воздействий как в отношении поставщиков, так и потребителей облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками безопасности элементов облачной инфраструктуры вследствие значительной распределённости облачной инфраструктуры. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)	Н						Данная технология не применяется в ИС
97	Угроза несогласованности правил доступа к большим данным	Угроза заключается в возможности предоставления ошибочного неправомерного доступа к защищаемой информации или, наоборот, возможности отказа в доступе к защищаемой информации легальным пользователям в силу ошибок, допущенных при делегировании им привилегий другими легальными пользователями хранилища больших данных. Данная угроза обусловлена недостаточностью мер по разграничению и согласованию доступа к информации различных пользователей в хранилище больших данных. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Угроза заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов. Данная угроза связана с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции сканирования портов и анализа сетевого трафика	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
				СТ	К	Репутационный Социальный	С		
99	Угроза обнаружения хостов	Угроза заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции анализа сетевого трафика	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
100	Угроза обхода некорректно настроенны х механизмов аутентифика ции	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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Акту альна я	
					Ц	Технологический Репутационный	С		
					Д	Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		
101	Угроза общедоступ ности облачной инфраструкт уры	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	С						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С	ПДН	Ц	Технологический Репутационный	В	Актуальная	
					Д	Технологический Репутационный	С		
				СТ	Ц	Технологический Экономический	В		
					Д	Технологический Экономический	С		
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 межсетевое 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.)	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Неактуальная	
				СТ	К	Социальный Репутационный	Н		

Продолжение таблицы 17

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
104	Угроза определения топологии вычислительной сети	<p>Угроза заключается в возможности определения нарушителем состояния сетевых узлов дискредитируемой системы (т.н. сканирование сети) для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз.</p> <p>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).</p> <p>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</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Неактуальная	
				СТ	К	Социальный Репутационный	Н		
105	Угроза отказа в загрузке входных данных неизвестного формата хранения больших данных	<p>Угроза заключается в возможности отказа хранилищем больших данных в приёме входных данных неизвестного формата от легального пользователя.</p> <p>Данная угроза обусловлена отсутствием в хранилище больших данных механизма самостоятельной (автоматической) адаптации к новым форматам данных.</p> <p>Реализация данной угрозы возможна при условии поступления запроса на загрузку в хранилище входных данных неизвестного формата</p>	Н					Данная технология не применяется в ИС	

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
106	Угроза отказа в обслуживании системы 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	Н						Данная технология не применяется в 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.). 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							Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
108	Угроза ошибки обновления гипервизора	<p>Угроза заключается в возможности дискредитации нарушителем функционирующих на базе гипервизора защитных механизмов, предотвращающих несанкционированный доступ к образам виртуальных машин, из-за ошибок его обновления.</p> <p>Данная угроза обусловлена зависимостью функционирования каждого виртуального устройства и каждого виртуализированного субъекта доступа, а также всей виртуальной инфраструктуры от работоспособности гипервизора.</p> <p>Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора: сбоях в процессе его обновления, обновлений, в ходе которых внедряются новые ошибки в код гипервизора, обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования либо других инцидентов безопасности информации</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
109	Угроза перебора всех настроек и параметров приложения	<p>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 конфигурации программы, достигая таких значений параметров путём перебора всех возможных комбинаций.</p> <p>Данная угроза обусловлена уязвимостями программного обеспечения, проявляющимися при его неправильной конфигурации.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение конфигурации программного обеспечения. При реализации данной угрозы, в отличие от других подобных угроз, нарушитель действует «вслепую» – простым путём перебора всевозможных комбинаций</p>	С	ПДН	Ц	Репутационный Технологический	С	Актуальная	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
110	Угроза перегрузки грид-системы вычислительными заданиями	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 от работоспособности гипервизора. Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора: сбоях в процессе его обновления, обновлений, в ходе которых внедряются новые ошибки в код гипервизора, обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования либо других инцидентов безопасности информации	Н						Данная технология не применяется в ИС
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. 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	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
111	Угроза передачи данных по скрытым каналам	<p>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.</p> <p>Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных.</p> <p>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; доступа к каналам передачи данных; посещении пользователем сайтов в сети Интернет и открытия электронных писем, содержащих скрытые пиксели</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Слциальный	Н		
113	Угроза перезагрузк и аппаратных и программно-аппаратных средств вычислительной техники	<p>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.</p> <p>Данная угроза обусловлена свойством оперативной памяти обнулять своё состояние при выключении и перезагрузке.</p> <p>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 на осуществление форсированной перезагрузки</p>	Н	ПДН	Ц	Технологический Репутационный	В	Актуальная	
					Д	Технологический Репутационный	С		
				СТ	Ц	Технологический Экономический	В		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасности информации	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
114	Угроза переполнени я целочисленн ых переменных	<p>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.</p> <p>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).</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя:</p> <p>сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных;</p> <p>возможности взаимодействия с входным интерфейсом дискредитируемого приложения</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	<p>Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информации, вводимой и выводимой на периферийные устройства, путём перехвата данных, обрабатываемых контроллерами периферийных устройств.</p> <p>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).</p> <p>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.</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
116	Угроза перехвата данных, передаваемых по вычислительной сети	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном (иногда в активном) режиме (т.е. «прослушивать сетевой трафик») для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы невидимым (скрытным) получателем перехватываемых данных. Кроме того, нарушитель может проводить исследования других типов потоков данных, например, радиосигналов. Данная угроза обусловлена слабостями механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибками конфигурации сетевого программного обеспечения. Реализация данной угрозы возможна в следующих условиях: наличие у нарушителя доступа к дискредитируемой вычислительную сети; неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информа ции	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
118	Угроза перехвата привилегированного процесса	<p>Угроза заключается в возможности получения нарушителем права управления процессом, обладающим высокими привилегиями (например, унаследованными от пользователя или группы пользователей, выполняющих роль администраторов дискредитируемой системы), для выполнения произвольного вредоносного кода с правами дискредитированного процесса.</p> <p>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.</p> <p>Реализация данной угрозы возможна при выполнении одного из условий:</p> <ul style="list-style-type: none"> 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 	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
119	Угроза перехвата управления гипервизором	<p>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.</p> <p>Данная угроза обусловлена наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью управления гипервизором</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
120	Угроза перехвата управления средой виртуализации	<p>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.</p> <p>Данная угроза обусловлена наличием у консоли средства управления виртуальной инфраструктурой, реализуемого в рамках одной из виртуальных машин, программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня управления виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью средства управления виртуальной инфраструктурой</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
121	Угроза повреждения системного реестра	Угроза заключается в возможности нарушения доступности части функционала или всей информационной системы из-за повреждения используемого в её работе реестра вследствие некорректного завершения работы операционной системы (неконтролируемая перезагрузка, возникновения ошибок в работе драйверов устройств и т.п.), нарушения целостности файлов, содержащих в себе данные реестра, возникновения ошибок файловой системы носителя информации или вследствие осуществления нарушителем деструктивного программного воздействия на файловые объекты, содержащие реестр. Данная угроза обусловлена слабостями мер контроля доступа к файлам, содержащим данные реестра, мер резервирования и контроля целостности таких файлов, а также мер восстановления работоспособности реестра из-за сбоев в работе операционной системы. Реализация данной угрозы возможна при одном из условий: возникновения ошибок в работе отдельных процессов или всей операционной системы; наличии у нарушителя прав доступа к реестру или файлам, содержащим в себе данные реестра	Н	ПДН	Ц	Репутационный Технологический	В	Акту альна я	
					Д	Репутационный Технологический	В		
				СТ	Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Акту альная я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
123	Угроза подбора пароля BIOS	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI путём входа в консоль BIOS/UEFI по паролю, подобранному программно или «вручную» с помощью методов тотального перебора вариантов или подбора по словарю. Данная угроза обусловлена слабостями механизма аутентификации, реализуемого в консолях BIOS/UEFI. Реализация данной угрозы возможна в одном из следующих случаев: 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Акту альная я	
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
124	Угроза подделки записей журнала регистрации событий	Угроза заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о не произошедших событиях) для введения в заблуждение её администраторов или сокрытия следов реализации других угроз. Данная угроза обусловлена недостаточностью мер по разграничению доступа к журналу регистрации событий безопасности. Реализация данной угрозы возможна в одном из следующих случаев: технология ведения журналов регистрации событий безопасности предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями; технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования, но нарушитель обладает привилегиями, необходимыми для осуществления записи в файлы журналов, а также специальными программными средствами, способными обрабатывать файлы журналов используемого в дискредитируемой системе формата	Н	ПДН	Ц	Репутационный Технологический	Н	Акту альна я	
				СТ	Ц	Технологический Экономический	С		
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	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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, 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	Н						Данная технология не применяется в ИС
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	Н		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	Н		
					Д	Технологический Экономический	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
128	Угроза подмены доверенного пользователя	<p>Угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента».</p> <p>Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника/получателя информации.</p> <p>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.</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Не актуальная	
				СТ	К	Репутационный Социальный	Н		
129	Угроза подмены резервной копии программного обеспечения BIOS	<p>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.</p> <p>Данная угроза обусловлена недостаточностью мер разграничения доступа и контроля целостности резервных копий программного обеспечения BIOS/UEFI.</p> <p>Реализация данной угрозы возможна в следующих условиях: нарушитель успешно подменил резервную копию программного обеспечения BIOS/UEFI; возникла необходимость восстановления предыдущей версии программного обеспечения BIOS/UEFI (данное условие может произойти как случайно, так и быть спровоцировано нарушителем)</p>	Н	ПДН	Ц	Репутационный Технологический	Н	Не актуальная	
				СТ	Ц	Технологический Экономический	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Социальный	С		
131	Угроза подмены субъекта сетевого доступа	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены в отправляемых дискредитируемым пользователем сетевых запросах сведений об отправителе сообщения. Данную угрозу можно охарактеризовать как «имитация действий сервера». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника информации. Реализация данной угрозы возможна при условии успешной выдачи себя нарушителем за законного отправителя (например, с помощью ложных фишинговых веб-сайтов). Ключевое отличие от «угрозы подмены содержимого сетевых ресурсов» заключается в том, что в данном случае нарушитель не изменяет оригинального содержимого электронного ресурса (веб-сайта, электронного письма), а только служебные сведения	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Технологический Репутационный	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Репутационный	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
132	Угроза получения предварительной информации об объекте защиты	<p>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.</p> <p>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.).</p> <p>Реализация данной угрозы возможна при условии получения информации о дискредитируемой системе с помощью хотя бы одного из следующих способов изучения дискредитируемой системы:</p> <p>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)</p> <p>анализ реакций системы на строковые URI-запросы (в т.ч. неверные SQL-запросы, альтернативные пути доступа к файлам).</p> <p>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</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угроз	Обоснование
133	Угроза получения сведений о владельце беспроводного устройства	<p>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.</p> <p>Данная угроза обусловлена слабостью защиты идентификационной информации беспроводных точек доступа при их подключении к сети Интернет.</p> <p>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</p>							Данная технология не применяется в ИС
135	Угроза потери и утечки данных, обрабатываемых в облаке	<p>Угроза заключается в возможности нарушения конфиденциальности, целостности и доступности защищаемой информации потребителей облачных услуг, обрабатываемой в облачной системе.</p> <p>Данная угроза обусловлена слабостями мер защиты информации, обрабатываемой в облачной системе.</p> <p>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</p>							Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
134	Угроза потери доверия к поставщику облачных услуг	<p>Угроза заключается в возможности снижения уровня защищённости и допущения дополнительных ошибок в обеспечении безопасности защищаемой в облачной системе информации из-за невозможности оттока у поставщика облачных услуг необходимых ресурсов в связи с потерей потребителями облачных услуг доверия к их поставщику.</p> <p>Данная угроза обусловлена тем, что из-за обнародования фактов об инцидентах информационной безопасности, связанных с поставщиком облачных услуг, происходит потеря доверия к такому поставщику со стороны потребителей облачных услуг, и, как следствие, возникает необходимость лавинообразного выделения поставщиком облачных услуг ресурсов (человеческих, технических, финансовых) для решения возникающих в данной ситуации задач (множественные консультации пользователей, экстренный пересмотр политик безопасности, модернизация системы защиты и др.), что не только может вызвать нехватку ресурсов для обеспечения текущего уровня защищённости информации, но и спровоцировать допуск «в спешке» новых ошибок.</p> <p>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</p>	С						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	<p>Угроза заключается в возможности допуска ошибок при копировании защищаемой информации при распределённом хранении данных на различных узлах хранилища больших данных вследствие несогласованности их работы, влекущих за собой невозможность осуществления легальным пользователем доступа к блокам или ко всей защищаемой информации.</p> <p>Данная угроза обусловлена слабостями механизмов репликации данных, реализованных в узлах хранилища больших данных.</p> <p>Реализация данной угрозы возможна в условиях отключения или вывода 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</p>	Н						Данная технология не применяется в ИС
137	Угроза потери управления облачными ресурсами	<p>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.</p> <p>Данная угроза обусловлена сложностью определения логического и физического местоположения облачных ресурсов, недостаточностью мер физического контроля доступа к хранилищам данных, резервного копирования и др., а также необходимостью учёта особенностей законодательства в области защиты информации стран, резидентами которых являются поставщики облачных услуг, выполняющих роль субподрядчиков по оказанию заказанных облачных услуг.</p> <p>Реализация данной угрозы возможна при условии, что выполнение требований к функционалу облачной системы затрудняется из-за правовых норм других стран, участвующих в трансграничной передаче облачного трафика</p>							Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
138	Угроза потери управления собственной инфраструктурой при переносе её в облако	<p>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.</p> <p>Данная угроза обусловлена невозможностью достоверной оценки потребителем облачных услуг реального уровня защищённости, обеспечиваемого поставщиком облачных услуг в отношении защищаемой информации потребителя облачных услуг, в связи с закрытостью для потребителей сведений о применяемых поставщиком облачных услуг технологиях, программных и технических решениях, а также конкретных параметрах настроек средств защиты информации.</p> <p>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)</p>	С						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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.)	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	В		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		
140	Угроза приведения системы в состояние «отказ в обслуживании»	Угроза заключается в возможности отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой 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 сетевых протоколов	Н	ПДН	Д	Репутационный Технологический	В	Акту альна я	
				СТ	Д	Технологический Экономический	В		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
141	Угроза привязки к поставщику облачных услуг	Угроза заключается в возможности возникновения трудно решаемых (или даже неразрешимых) проблем технического, организационного, юридического или другого характера, препятствующих осуществлению потребителем облачных услуг смены их поставщика. Данная угроза обусловлена отсутствием совместимости между форматами данных и программными интерфейсами, используемыми в облачных инфраструктурах различных поставщиков облачных услуг. Реализация данной угрозы возможна при условии использования поставщиком облачных услуг нестандартного программного обеспечения или формата образов виртуальных машин и отсутствием средств преобразования образа виртуальной машины из используемого им формата в другой (используемый другим поставщиком)	Н						Данная технология не применяется в ИС
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							Данная технология не применяется в ИС

Продолжение таблицы 17

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
143	Угроза программного вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	<p>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.</p> <p>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).</p> <p>Реализация данной угрозы возможна при наличии у нарушителя прав на отправку команды или специально сформированных входных данных на средства хранения, обработки и (или) ввода/вывода/передачи информации</p>	С	ПДН	Ц	Репутационный Технологический	В	Актуальна	
					Д	Репутационный Технологический	В		
				СТ	Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информа ции	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
144	Угроза программно го 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Акту альна я	
					Ц	Технологический Репутационный	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технолгический Репутационный	С		
145	Угроза прямого обращения к памяти вычислитель ного поля суперкомпьютера	Угроза заключается в возможности осуществления процессом нарушителя, функционирующем в вычислительном поле суперкомпьютера, считывания защищаемых данных из оперативной памяти, выделенной для параллельного (дискредитируемого) процесса, с использованием операций удалённого прямого доступа к памяти. Данная угроза обусловлена слабостями протокола прямого доступа к оперативной памяти, с помощью которого выполняется обращение к сегменту памяти, выделенному для удалённого параллельного процесса, функционирующего в вычислительном поле суперкомпьютера. Реализация данной угрозы возможна при условии успешного осуществления нарушителем доступа к входным/выходным данным параллельных процессов в вычислительном поле суперкомпьютера	С						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
146	Угроза пропуска проверки целостности программно го обеспечения	<p>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.</p> <p>Данная угроза обусловлена слабостями механизмов проверки целостности файлов программного обеспечения и/или проверки подлинности источника их получения.</p> <p>Реализация данной угрозы возможна при условии успешного использования обманных техник одного из следующих методов:</p> <p>«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);</p> <p>«автоматического метода» – нарушитель осуществляет деструктивное воздействие переадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер</p>	Н	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С						Данная технология не применяется в 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» 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							Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
149	Угроза сбоя обработки специальными 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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
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)	С	ПДН	Д	Репутационный Технологический	С	Акту альна я	
				СТ	Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Не актуальная	
				СТ	К	Репутационный Социальный	Н		
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	Н		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на дискредитируемую систему большим объемом сетевого трафика, генерируемого сторонними серверами в ответ на сетевые запросы нарушителя, сформированные от имени дискредитируемой системы. Генерируемый сторонними серверами сетевой трафик значительно превышает объем 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	Н	ПДН	Д	Репутационный Технологический	С	Акту альна я	
				СТ	Д	Технологический Экономический	С		
154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Угроза заключается в возможности внесения уязвимостей в программное обеспечение BIOS/UEFI в ходе его обновления, которые могут быть использованы в дальнейшем для приведения компьютера в состояние «отказ в обслуживании», несанкционированного изменения конфигурации BIOS/UEFI или выполнения вредоносного кода при каждом запуске компьютера. Данная угроза обусловлена слабостями мер контроля отсутствия уязвимостей в только что вышедших версиях обновления программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Технологический	С		
					Д	Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
155	Угроза утраты вычислительных ресурсов	<p>Угроза заключается в возможности отказа легитимному пользователю в выделении ресурсов для обработки его запросов из-за истощения нарушителем свободных ресурсов в системе, осуществлённого путём их несанкционированного исключения из общего пула ресурсов на основе техник «утечки ресурсов» или «выделения ресурсов».</p> <p>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.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя:</p> <p>сведений о формате и параметрах деструктивных воздействий на систему, приводящих к исключению («утечки» или «выделению») свободных ресурсов из общего пула ресурсов дискредитируемой системы;</p> <p>привилегий, достаточных для осуществления деструктивных воздействий («утечки» или «выделения») в дискредитируемой системе;</p> <p>отсутствия 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</p>	Н	ПДН	Д	Репутационный Технологический	С	Актуальная	
				СТ	Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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	Н	ПДН	К	Репутационный Ущерб субъекту ПДН	С	Акту альна я	
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	С		
					Д	Технологический Экономический	Н		
157	Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угроза заключается в возможности умышленного вывода из строя внешним нарушителем средств хранения, обработки и (или) ввода/вывода/передачи информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Н	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
158	Угроза форматирования носителей информации	Угроза заключается в возможности утраты хранящейся на формируемом 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.	Н	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
159	Угроза «форсированного веб-браузинга»	Угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации «ручного ввода» в адресную строку веб-браузера определённых адресов веб-страниц и осуществления принудительного перехода по дереву веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
				СТ	К	Репутационный Социальный	С		

Продолжение таблицы 17

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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.)	Н	ПДН	К	Репутационный Ущерб субъекту ПДН	В	Актуальная	
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Д	Технологический Экономический	Н		
161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Угроза заключается в возможности возникновения ситуации типа «отказ в обслуживании» со стороны вычислительного поля суперкомпьютера. Данная угроза обусловлена слабостями мер контроля за распределением вычислительных ресурсов суперкомпьютера при обработке задачи несколькими процессорами. Реализация данной угрозы возможна при условии выполнения суперкомпьютером специфичных вычислительных задач, в ходе которых генерируются межпроцессорные сообщения с большой интенсивностью	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
162	Угроза эксплуатации и цифровой подписи программного кода	Угроза заключается в возможности повышения нарушителем привилегий в системах, использующих цифровую подпись кода в качестве связующей информации между программой и её привилегиями, путём дискредитации механизма подписывания программного кода. Данная угроза обусловлена слабостями в механизме подписывания программного кода. Реализация данной угрозы возможна при следующих условиях: дискредитируемый программный код написан с помощью фреймворка (framework), поддерживающего подписывание программного кода; дискредитируемый программный код подписан вендором (поставщиком программного обеспечения); нарушитель имеет возможность внедрить программный код в дискредитируемый компьютер	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
163	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 уровне 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»	Н						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
164	Угроза перехвата исключения/сигнала из привилегированного блока функций	<p>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.</p> <p>Данная угроза обусловлена тем, что вызов программных функций в привилегированном режиме подразумевает отключение для них механизмов разграничения доступа.</p> <p>Реализация данной угрозы возможна при следующих условиях:</p> <p>дискредитируемая программа, написана на языке программирования, поддерживающего механизм привилегированных блоков (например, Java);</p> <p>в дискредитируемой программе вызов привилегированных блоков осуществлён небезопасным способом (использовано публичное объявление внутренних функций, использована генерация исключений из привилегированного блока);</p> <p>нарушитель обладает правами, достаточными для перехвата программных исключений в системе</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
165	Угроза включения в проект не достоверно испытанных компонентов	Угроза заключается в возможности нарушения безопасности защищаемой информации вследствие выбора для применения в системе компонентов не в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др. Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии выбора применения в системе компонентов по цене, разрекламированности и др.	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	Н		
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)	С	ПДН	Д	Репутационный Технологический	С	Акту альна я	
				СТ	Д	Технологический Экономический	В		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Угроза заключается в возможности нарушения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест (намеренно или при случайном перенаправлении) сайтов с неблагонадёжным содержимым и запускаемыми с привилегиями дискредитированных пользователей. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов с неблагонадёжным содержимым	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Акту альная я	
					Ц	Технологический Репутационный	В		
					Д	Технологический	В		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		
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, 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; наличия у нарушителя сведений об адресе электронной почты, с которым связана учётная запись дискредитируемого пользователя для доступа к сетевым сервисам	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альная я	
					Д	Технологический Репутационный	В		
				СТ	К	Репутационный Социальный	С		
					Д	Технологический	В		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Акту альная я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	Н		
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	Н	ПДН	Д	Репутационный Технологический	С	Акту альная я	
				СТ	Д	Технологический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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, 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. 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	Н	ПДН	Д	Репутационный Технологический	С	Акту альна я	
				СТ	Д	Технологический	В		
172	Угроза распространения «почтовых червей»	Угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми при получении пользователями системы электронных писем, содержащих вредоносную программу типа «почтовый червь», а также невольного участия в 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический	С		
					Д	Технологический	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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, онлайн-сервисы отправки SMS-сообщений, онлайн-сервисы голосования и др.	Н	ПДН	Д	Репутационный Технологический	С	Актуальная	
				СТ	Д	Технологический	С		
174	Угроза «фарминга»	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией пользователя путём скрытного перенаправления пользователя на поддельный сайт, 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
175	Угроза «фишинга»	<p>Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём убеждения его с помощью методов социальной инженерии (в т.ч. посылкой целевых писем (т.н. spear-phishing attack), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений (fake offers) или различных приложений (fake apps)) зайти на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть заражённое вложение в письме.</p> <p>Данная угроза обусловлена недостаточностью знаний пользователей о методах и средствах «фишинга».</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя:</p> <ul style="list-style-type: none"> 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.). <p>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)</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
				СТ	К	Репутационный Социальный	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушения	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Угроза заключается в возможности приведения системы в состояние «отказ в обслуживании» или нарушения штатного режима функционирования из-за временной задержки в системах реального времени, вносимой в процессы передачи и обработки защищаемой информации средствами защиты информации, вызванной необходимостью обработки передаваемой/обрабатываемой информации на предмет выявления и нейтрализации угроз безопасности информации. На реализацию данной угрозы влияет не только номенклатура применяемых средств защиты информации, параметры их настройки, объём передаваемой/обрабатываемой информации, а также текущая активность внешних нарушителей, программные воздействия которых обрабатываются средствами защиты информации	Н	ПДН	Д	Репутационный Технологический	Н	Актуальна	
				СТ	Д	Технологический	С		
177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Угроза заключается в возможности возникновения ошибок в работе системы вследствие отсутствия (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора, средства учёта нижних/верхних пределов скорости и направления реакции оператора, схемы реагирования на двойное нажатие клавиш при вводе обычных и критических данных, процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.). 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 требованиями и фактическим уровнем обнаружения и исправления ошибок	Н	ПДН	Ц	Репутационный Технологический	Н	Актуальна	
					Д	Репутационный Технологический	Н		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	Н		
179	Угроза несанкционированной модификации и 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	Н	ПДН	Ц	Репутационный Технологический	С	Актуальная	
				СТ	Ц	Технологический Экономический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
180	Угроза отказа подсистемы обеспечения температурн ого 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	С	ПДН	Д	Репутационный Технологический	В	Акту альна я	
				СТ	Д	Технологический	В		
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	С	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
				СТ	Ц	Технологический Экономический	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
182	Угроза физического устаревания аппаратных компонентов	Угроза заключается в возможности нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозионных субстанций). Возможность реализации данной угрозы возрастает при использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем	Н	ПДН	Д	Репутационный Технологический	С	Актуальна	
				СТ	Д	Технологический	С		
183	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Угроза заключается в возможности осуществления нарушителем сбора и анализа информации, обрабатываемой с помощью мобильного устройства, за счёт использования специального программного обеспечения, встраиваемого пользователем в системное программное обеспечение мобильного устройства, а также встраиваемого в мобильные программы под видом программной платформы для их разработки другими компаниями. Данная угроза обусловлена наличием в мобильном устройстве множества каналов передачи данных, а также сложностью контроля потоков информации в таком устройстве. Реализация данной угрозы возможна при условии использования мобильных устройств пользователями. В качестве собираемой информации могут выступать: персональные данные пользователя и контактирующих с ним лиц (пол, возраст, религиозные и политические взгляды и др.); информация ограниченного доступа (история браузера, список контактов пользователя, история звонков и др.); видеоданные, снимаемые видеокамерами мобильного устройства; аудиоданные, снимаемые микрофоном устройства	С						Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
184	Угроза перехвата управления автоматизированной системой управления технологическими процессами	<p>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.</p> <p>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.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с автоматизированной системой управления технологическими процессами. Реализация данной угрозы может привести к:</p> <p>блокированию или искажению (некорректность выполнения) алгоритмов отработки заданий управления технологическими процессами, непосредственного управления оборудованием предприятия;</p> <p>нарушению штатного хода технологических процессов;</p> <p>частичному или полному останову технологических процессов без (или с) выхода(-ом) оборудования из строя;</p> <p>аварийной ситуации в критической системе информационной инфраструктуры</p>							Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	С		
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	Н	ПДН	Ц	Репутационный Технологический	С	Актуальная	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	Н		
					Д	Технологический	Н		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		
188	Угроза подмены программного обеспечения	Угроза заключается в возможности осуществления нарушителем внедрения в систему вредоносного программного обеспечения за счёт загрузки и установки вредоносного программного обеспечения, скрытого под видом легитимного свободно распространяемого программного обеспечения. 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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информа ции	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
189	Угроза маскировани я действий вредоносног о 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	С	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	Н		
					Д	Технологический	С		
190	Угроза внедрения вредоносног о кода за счет посещения зараженных сайтов в сети Интернет	Угроза заключается в возможности осуществления нарушителем внедрения вредоносного кода в компьютер пользователя при посещении зараженных сайтов. Нарушитель выявляет наиболее посещаемые пользователем сайты, затем их взламывает и внедряет в них вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты, а также отсутствием правил межсетевого экранирования. Реализация данной угрозы возможна при: неограниченном доступе пользователя в сеть Интернет; наличии у нарушителя сведений о сайтах, посещаемых пользователем	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Угроза заключается в возможности осуществления нарушителем заражения системы путем установки дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты. Реализация данной угрозы возможна при: применении пользователем сторонних дистрибутивов; отсутствии антивирусной проверки перед установкой дистрибутива	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		
192	Угроза использования уязвимых версий программного обеспечения	Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения. Данная угроза обусловлена слабостями механизмов анализа программного обеспечения на наличие уязвимостей. Реализация данной угрозы возможна при отсутствии проверки перед применением программного обеспечения на наличие в нем уязвимостей	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	В		
				СТ	К	Репутационный	В		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
				СТ	К	Репутационный Социальный	В		
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	В						Не применима к рассматриваемой системе

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	В	ПДН	Ц	Технологический Репутационный	В	Актуальна	
				СТ	Ц	Технологический Экономический	В		
196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Угроза заключается в возможности использования вредоносной программы для контроля списка приложений, запущенных на мобильном устройстве. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносных программ (отсутствие контроля разрешенного программного обеспечения). Реализация данной угрозы возможна при условии, что вредоносная программа внедрена на мобильном устройстве и непреднамеренно запущена самим пользователем	В						Не применима к рассматриваемой системе

Продолжение таблицы 17

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угроз	Обоснование
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
				СТ	К	Репутационный Социальный	С		
198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Угроза заключается в возможности скрытного создания внедренной вредоносной программой учетных записей с правами администратора с целью последующего их использования для несанкционированного доступа к пользовательской информации и к настройкам программного обеспечения, установленного на инфицированном компьютере. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения). Кроме того, данная угроза обусловлена недостаточностью мер по разграничению доступа (контроль создания учетных записей пользователей). Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт	С	ПДН	Ц	Репутационный Технологический	С	Актуальная	
				СТ	Ц	Технологический Экономический	С		

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Угроза заключается в возможности управления мобильным устройством и запущенными на нем приложениями от имени легального пользователя за счет передачи этих команд через виртуальных голосовых ассистентов (например, через Siri для iPhone). Данная угроза обусловлена проблемами аутентификации пользователя, в частности по Voice ID. Голосовой ассистент не может быть полностью уверен в том, что обращающийся к нему голос принадлежит владельцу устройства, поэтому для удобства пользователей и гарантии срабатывания устанавливается низкая чувствительность Voice ID. Это позволяет нарушителю использовать записанную на диктофон речь владельца мобильного устройства. Реализация данной угрозы возможна при условии, что виртуальный голосовой ассистент находится в активном состоянии (то есть, не отключен) и установлена низкая чувствительность голосового идентификатора							Не применима к рассматриваемой системе
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							Не применима к рассматриваемой системе

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Угроза заключается в возможности утечки пользовательских данных за счет использования реализованной в браузерах функции автоматического заполнения 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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Акту альна я	
				СТ	К	Репутационный Социальный	В		
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 вредоносной программы, способной запустить виртуальную машину и установить в эту виртуальную машину приложение							Не применима к рассматриваемой системе

Продолжение таблицы 17

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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, 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							Не применима к рассматриваемой системе
204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Угроза заключается в возможности несанкционированного изменения вредоносной программой значений параметров контроля и управления исполнительными устройствами в программируемых логических контроллерах после ее проникновения и авторизации на данных устройствах. Реализация угрозы обусловлена возможностью вредоносной программы обнаруживать в сети программируемые логические контроллеры, проникать и функционировать в операционной системе программируемых логических контроллеров, а также недостатками механизмов аутентификации. Реализация данной угрозы возможна при условии, что существует возможность доступа к элементам автоматизированной системы управления технологическими процессами по сети Интернет							Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	Н	ПДН	Д	Репутационный Технологический	С	Актуальна	
				СТ	Д	Технологический	С		
206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Угроза заключается в прекращении работы оборудования с ЧПУ, вызванном изменением геолокационной информации о данном оборудовании. Угроза обусловлена геолокационной привязкой оборудования с ЧПУ к конкретной географической координате при пуско-наладочных работах. Угроза реализуется при условии перемещения оборудования с ЧПУ и приводит к невозможности его дальнейшей эксплуатации							Данная технология не применяется в ИС

Продолжение таблицы 17

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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							Данная технология не применяется в ИС

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потенци ал нарушит еля	Вид обраба тывае мой инфор мации	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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 программы; мер по ограничению программной среды, что позволяют нарушителю осуществлять бесконтрольный запуск программных компонентов.	Внутренний с низким потенциалом	ПДН	Д	Технологический Репутационный	С	Акту альна я	
				СТ	Д	Технологический Экономический	С		
			Внутренний со средним потенциалом	ПДН	Д	Технологический Репутационный	В		
				СТ	Д	Технологический Экономический	В		
			Внешний с низким	ПДН	Д	Технологический Репутационный	С		
				СТ	Д	Технологический Экономический	С		
			Внешний со средним	ПДН	Д	Технологический Репутационный	В		
				СТ	Д	Технологический Экономический	В		

Продолжение таблицы 17

№ угр озы	Название угрозы	Описание угрозы	Потенци ал нарушит еля	Вид обраба тывае мой инфор мации	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
209	Угроза несанкциони рованного доступа к защищаемой памяти ядра процессора	<p>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.</p> <p>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:</p> <p>1) отсутствие проверки прав доступа процесса к читаемым областям при спекулятивном выполнении операций, в том числе при чтении из оперативной памяти;</p> <p>2) отсутствие очистки кэша от результатов ошибочного спекулятивного исполнения;</p> <p>3) хранение данных ядра операционной системы в адресном пространстве процесса.</p> <p>Реализация данной угрозы возможна из-за наличия процессоров, имеющих аппаратные уязвимости и отсутствия соответствующих обновлений</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		

159

№ угр озы	Название угрозы	Описание угрозы	Потенци ал нарушит еля	Вид обраба тывае мой инфор мации	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
210	Угроза нарушения работы информацион ной системы, вызванного обновлением используемого в ней программного обеспечения	<p>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.</p> <p>Угроза обусловлена наличием критических ошибок, дефектов, уязвимостей в используемом программном обеспечении информационной системы.</p> <p>Реализация данной угрозы возможна при условии установки обновлений на программно-аппаратные компоненты информационной системы</p>	В	<div>ПДН</div> <div>Ц</div> <div>Д</div> <div>СТ</div> <div>Д</div>	<div>Ц</div> <div>Д</div> <div>Ц</div> <div>Д</div>	<div>Технологический Репутационный</div> <div>Технологический Репутационный</div> <div>Технологический Экономический</div> <div>Технологический</div>	<div>В</div> <div>В</div> <div>В</div> <div>В</div>	Акту альна я	
211	Угроза использования непроверенны х пользовательс ких данных при формировании конфигурацио нного файла, используемого программным обеспечением администриро вания информацион ных систем	<p>Угроза заключается в возможности деструктивного воздействия на информационную систему и обрабатываемую ею информацию в результате работы программного обеспечения, используемого для администрирования информационных систем.</p> <p>Данная угроза связана со слабостями процедуры проверки пользовательских данных, используемых при формировании конфигурационного файла для программного обеспечения администрирования информационных систем.</p> <p>Реализация данной угрозы возможна в случае, если в информационной системе используется программное обеспечение администрирования информационных систем, которое в качестве исходных данных использует конфигурационные файлы, сформированные на основе пользовательских данных</p>	Н	<div>ПДН</div> <div>Ц</div> <div>СТ</div> <div>Ц</div>	<div>К</div> <div>Ц</div> <div>К</div> <div>Ц</div>	<div>Ущерб субъекту ПДН Репутационный</div> <div>Технологический Репутационный</div> <div>Репутационный Социальный</div> <div>Технологический Экономический</div>	<div>В</div> <div>С</div> <div>С</div> <div>В</div>	Акту альна я	

Продолжение таблицы 17

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушения	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	В		
				СТ	К	Репутационный Социальный	В		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		
213	Угроза обхода многофакторной аутентификации	Угроза заключается в возможности обхода многофакторной аутентификации путем внедрения вредоносного кода в дискредитируемую систему и компоненты, 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	В	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Модель угроз в виде документа представлена в Приложении Г.

8 Возможность использования разработанной модели угроз информационной системы «Веб-сайта Правительства Пензенской области» для идентификации актуальных угроз информационных систем веб-сайтов исполнительных органов государственной власти и органов местного самоуправления Пензенской области.

Данная модель угроз может быть применена к аналогичным информационным системам, находящимся в пользовании у Правительства Пензенской области. В частности это относится к следующим информационным системам:

- «веб-сайт Министерства здравоохранения Пензенской области»;
- «веб-сайт Министерства лесного, охотничьего хозяйства и природопользования Пензенской области»;
- «веб-сайт Министерства образования Пензенской области»;
- «веб-сайт Министерства промышленности, транспорта и инновационной политики Пензенской области»;
- «веб-сайт Министерства сельского хозяйства Пензенской области»;
- «веб-сайт Министерства строительства и дорожного хозяйства Пензенской области»;
- «веб-сайт Министерства труда, социальной защиты и демографии Пензенской области»;
- «веб-сайт Министерства физической культуры и спорта Пензенской области»;
- «веб-сайт Министерства финансов Пензенской области»;
- «веб-сайт Министерства экономики Пензенской области»;
- «веб-сайт Министерства культуры и туризма Пензенской области»;
- «веб-сайт Управления ветеринарии Пензенской области»;

- «веб-сайт Управления государственной инспекции в жилищной, строительной сферах и по надзору за техническим состоянием самоходных машин и других видов техники Пензенской области»;
- «веб-сайт Управления жилищно-коммунального хозяйства и гражданской защиты населения Пензенской области»;
- «веб-сайт Управления ЗАГС Пензенской области»;
- «веб-сайт Управления цифрового развития, информационных технологий и связи Пензенской области»;
- «веб-сайт Управления общественной безопасности и обеспечения деятельности мировых судей в Пензенской области»;
- «веб-сайт Управления по регулированию контрактной системы и закупкам Пензенской области»;
- «веб-сайт Управления по регулированию тарифов и энергосбережению Пензенской области»;
- «веб-сайт Департамента государственного имущества Пензенской области»;
- «веб-сайт Департамента градостроительства и архитектуры Пензенской области»;
- «веб-сайт Департамента информационной политики и средств массовой информации Пензенской области»;
- «веб-сайт Комитета Пензенской области по охране памятников истории и культуры»;
- «веб-сайт Комитета по делам архивов Пензенской области»;
- «веб-сайт Представительства Правительства Пензенской области при Правительстве РФ»;
- ко всем веб-сайтам органов местного самоуправления Пензенской области.

Применимость модели угроз информационной системы «веб-сайт Правительства Пензенской области» к аналогичным системам обуславливается следующими пунктами:

- данные информационные системы размещены в пределах одного здания;
- назначение данных ИС аналогично;
- данные ИС размещены на одном сервере с виртуальным разграничением между собой;
- данные ИС обслуживаются одинаковым персоналом;
- данные ИС подключены к одинаковым техническим средствам и сетям;
- модели нарушителей данных ИС являются аналогичными;
- активы данных ИС являются аналогичными.

9 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.

Заболевания сердечно-сосудистой системы является частой причиной потери трудоспособности а также смерти взрослого населения во многих уголках мира. Среди болезней сердечно-сосудистой системы наиболее распространены артериальная гипертония и ишемическая болезнь сердца.

Многочисленные исследования показали, что ускорение жизни, возникновение сложных трудовых процессов влияют в первую очередь на возрастание нервно-эмоционального напряжения. Но помимо этого часть повседневной жизни человека наоборот упрощается, к примеру повсеместное использование автомобилей позволило человеку проводить больше времени в сидячем положении, что существенно сказалось на системе кровообращения, так как в организме происходит застаивание крови.

Долгосрочные исследования и эксперименты показали, что аномалии в работе сердечно-сосудистой системы как одной из важнейших систем в организме человека, фиксируются в основном при воздействии различных профессионально-производственных факторов химической и физической природы. Вместе с тем особое значение системы кровообращения в общем аппарате адаптации организма человека к воздействию экзо и эндогенных факторов, высокая частота заведомо неблагоприятных влияний на сердечно-сосудистую систему ряда непрофессиональных факторов и неспецифичность отклонений затрудняют установление роли отдельных факторов в возникновении указанных нарушений. Многими исследователями показано, что нервно-эмоциональное перенапряжение является одной из ведущих причин роста числа сердечно-сосудистых заболеваний.

На основании изучения заболеваемости сердечно-сосудистой системы инженеров, программистов, специалистов по информационной безопасности а

также других профессий со схожими условиями труда, Береславская Е.Б. В своих работах отмечает что в силу высокого эмоционально-нервного напряжения у пациентов происходит возникновение большого числа заболеваний сердечно-сосудистой системы. В частности у специалистов по защите информации наблюдения показали повышенное число заболеваний связанных с артериальной гипертонией.

Гипертония характеризуется повышенным артериальным давлением вследствие нарушения сложных механизмов нервной и эндокринно-ферментативной регуляции. Данное заболевание может быть вызвано не только вследствие напряжённого эмоционально-нервного состояния человека, но и также в случае возникновения психических травм, перенапряжения как умственного так и физического, длительных воздействий отрицательных эмоций. Также следует выделить, что вследствие преобладания сидячего образа в рабочей деятельности у специалисты по защите информации предрасположены к появлению избыточного веса, который в свою очередь предрасполагает к появлению гипертонической болезни.

Заболевания сердечно-сосудистой системы носят волнообразный характер, то есть пациент периодически испытывает периоды ухудшения, которые сменяются спокойными этапами, когда болезнь не даёт о себе знать.

Лечебная физкультура является одним из основных способов предотвращения возникновения заболеваний сердечно-сосудистой системы. Но лечебная физкультура также полезна уже при наступлении заболевания, правда в таком случае желательно проконсультироваться с врачом и строго следовать его рекомендациям.

Занятия лечебной физкультурой желательно начинать в период улучшения состояния. При начальной стадии заболеваний следует произвести упор в лечебную гимнастику, спокойную ходьбу, плавание, катание на лыжах а также лёгкие спортивные игры, наподобие настольного тенниса и бадминтона. Занятия стоит продолжать до момента ухудшения состояния здоровья,

постепенно увеличивая нагрузку. При ухудшении самочувствия рекомендуется снизить нагрузку на организм (эмоциональную и физическую).

При более серьёзном течении заболевания рекомендуется отказаться от спортивных игр, катания на лыжах и снизить нагрузку при плавании. Ходьба и лечебная гимнастика рекомендуются по-прежнему.

Людам, подверженным высоким психологическим нагрузкам рекомендуется производить периодическую лечебную зарядку на рабочем месте, для снижения вероятности возникновения заболеваний сердечно-сосудистой системы.

В заключение хочется сказать, что работа специалиста по защите информации напрямую связана с постоянным напряжением, вследствие чего для профилактики заболеваний сердечно-сосудистой системы специалисту необходимо производить периодическую зарядку, а в свободное время умеренно заниматься спортом а при появлении первых признаков заболеваний обращаться к компетентным врачам.

Заключение

В процессе выполнения выпускной квалификационной работы было проведено описание информационной системы «Веб-сайт Правительства Пензенской области» а также её структурно-функциональных характеристик.

По результатам анализа информационной системы была произведена идентификация активов информационной системы, по результатам которой разработан соответствующий нормативный документ.

Опираясь на описание информационной системы, её структурно-функциональные характеристики а также идентифицированные активы, была разработана модель нарушителя и модель угроз безопасности информации. Для данных моделей были разработаны соответствующие документы.

Финальным этапом выпускной квалификационной работы выступает оценка возможности использования разработанной модели угроз информационной системы веб сайта Правительства Пензенской области для идентификации актуальных угроз информационных систем веб-сайтов исполнительных органов государственной власти и органов местного самоуправления Пензенской области.

Таким образом, задачи, поставленные в техническом задании выполнены в полном объёме.

Список используемых источников

1 Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ [Электронный ресурс] / Принят Государственной Думой 8 июля 2006 года, одобрен Советом Федерации 14 июля 2006 года. Ред. от 31.12.2017. // Справочная правовая система КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 28.02.2019).

2 Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации [Электронный ресурс] / Утв. постановлением Правительства РФ от 15 сентября 2008 г. № 687. // Информационно-правовой портал ГАРАНТ. URL: <https://base.garant.ru/193875/> (дата обращения: 28.02.2019).

3 Постановление правительства Российской Федерации № 211 [Электронный ресурс] / Утв. Постановление Правительства РФ от 21 марта 2012г. N211 // Информационно-правовой портал ГАРАНТ. URL: <https://base.garant.ru/70152982/> (дата обращения 28.02.2019)

4 Постановление правительства Российской Федерации №781 [Электронный ресурс] / Принят Постановление Правительства РФ 17 ноября 2007г. N781 // Информационно-правовой портал ГАРАНТ. URL: <https://base.garant.ru/192223/> (дата обращения 28.02.2019)

5 Приказ ФСБ РФ и Федеральной службы по техническому и экспортному контролю N 416/489 [Электронный ресурс] / Утв. ФСБ РФ и Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. // Информационно-правовой портал ГАРАНТ. URL: <https://base.garant.ru/70152982/> (дата обращения 28.02.2019)

6 Приказ Минкомсвязи РФ N 104 [Электронный ресурс] / Утв. Минкомсвязи РФ от 25 августа 2009 г. // Информационно-правовой портал

ГАРАНТ. URL: <http://ivo.garant.ru/#/document/196351/paragraph/1:1> (дата обращения 28.02.2019)

7 Приказ Федеральной службы по техническому и экспортному контролю N 17 [Электронный ресурс] / Утв. Федеральной службы по техническому и экспортному контролю РФ от 11 февраля 2013 г. // Информационно-правовой портал ГАРАНТ. URL: <https://base.garant.ru/70391358/> (дата обращения 28.02.2019)

8 Методический документ Методика определения угроз безопасности информации в информационных системах [Электронный ресурс] / Утв. Федеральной службы по техническому и экспортному контролю РФ // Информационно портал Федеральной службы по техническому и экспортному контролю URL: <https://fstec.ru/component/attachments/download/812> (дата обращения 03.06.2019)

9 Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю РФ [Электронный ресурс] / Утв. Федеральной службы по техническому и экспортному контролю РФ // Информационно портал Федеральной службы по техническому и экспортному контролю URL: <https://bdu.fstec.ru/threat> (дата обращения 03.06.2019)

10 Федеральный закон Об информации, информационных технологиях и о защите информации № 149 [Электронный ресурс] / Принят государственной думой от 8 июля 2006 г. // Информационно-правовой портал Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 03.06.2019)

11 Федеральный закон Об электронной подписи № 63 [Электронный ресурс] / Принят государственной думой от 25 марта 2011 г. // Информационно-правовой портал Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения 03.06.2019)

12 Постановление Правительства РФ № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс] / Принят государственной думой от 1 ноября 2012 г. // Информационно-правовой портал Консультант Плюс. URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=137356&fld=134&dst=1000000001,0&rnd=0.07213286140546349#08183625012147384> (дата обращения 03.06.2019)

13 Федеральный закон №8 Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления [Электронный ресурс] / Принят государственной думой от 21 января 2009 г. // Информационно-правовой портал Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_84602/ (дата обращения 03.06.2019)

14 Закон Пензенской области О Правительстве Пензенской области №906 [Электронный ресурс] / Принят законодательным собранием Пензенской области 21 декабря 2005г. // Электронный фонд правовой и нормативно-технической документации. URL: <http://docs.cntd.ru/document/949101642> (дата обращения 03.06.2019)

Приложение А
(обязательное)

Перечень активов

УТВЕРЖДАЮ

(должность)

(подпись) (Фамилия)

« 1 » мая 2019 г.

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ И ВСПОМОГАТЕЛЬНЫХ АКТИВОВ
ИНФОРМАЦИОННОЙ СИСТЕМЫ «ВЕБ-САЙТ ПРАВИТЕЛЬСТВА ПЕНЗЕНСКОЙ
ОБЛАСТИ»

1 Общие положения

Перечень информационных и вспомогательных активов был составлен в рамках создания модели угроз для информационной системы «Веб-сайт Правительства Пензенской области» по результатам экспертной оценки.

Перечень информационных и вспомогательных активов подлежит обязательной актуализации по прошествии каждые 3 лет, а также при существенном изменении информационной системы «Веб-сайт Правительства Пензенской области».

Ответственным за актуализацию перечня информационных и вспомогательных активов назначается начальник Управления информационной безопасности Андреев А.Б.

2 Перечень активов

Информационные активы с высоким уровнем ценности:

- персональные данные клиентов ИС;
- идентификационные данные клиентов ИС.

Информационные активы со средним уровнем ценности:

- обращения граждан;
- служебная информация.

Информационные активы с низким уровнем ценности отсутствуют.

Вспомогательные активы с высоким уровнем ценности:

- сетевое оборудование;
- сервер Веб-сайта правительства Пензенской области;
- сервер системы электронного документооборота Пензенской области;
- среда виртуализации Oracle VM VirtualBox Enterprise.

Вспомогательные активы со средним уровнем ценности:

— АРМ сотрудников.

Вспомогательные активы с низким уровнем ценности отсутствуют.

(Должность) Правительства Пензенской области

« 1 » мая 2019 г. _____ (Фамилия)

Начальник отдела информационной безопасности

« 1 » мая 2019 г. _____ (Фамилия)

Приложение Б

(обязательное)

Акт классификации информационной системы «Веб-сайт Правительства Пензенской области»

Комиссия, назначенная Распоряжением №214 от «1» февраля 2019 года «О комиссии по категорированию защищаемых помещений, определению уровней защищенности персональных данных в информационных системах персональных данных, классификации государственных информационных систем и автоматизированных информационных систем, предназначенных для обработки служебной информации (служебной тайны)», провела классификацию информационной системы «Веб-сайт Правительства Пензенской области» (далее – ИС «Веб-сайт Правительства Пензенской области») установила:

1 Основание для проведения классификации

ИС «Веб-сайт Правительства Пензенской области» находится в пользовании у государственного органа исполнительной власти Правительство Пензенской области в соответствии с ФЗ-149 от 27.07.2016 [10] данная ИС является государственной, т. к. она создана в целях реализации полномочий государственных органов.

ИС «Веб-сайт Правительства Пензенской области» является информационной системой общего пользования согласно федеральному закону от 06.04.2011 N 63-ФЗ (ред. от 10.07.2012) "Об электронной подписи"[11], так как участники электронного взаимодействия составляют неопределенный круг лиц, а также в пользовании данной ИС им не может быть отказано.

Классификация ИС «Веб-сайт Правительства Пензенской области»

осуществляется в соответствии с приказом ФСТЭК России от 11 февраля 2013 года №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Приказ ФСТЭК №17)[7].

Определение уровня защищенности персональных данных, при их обработке в ИС «Веб-сайт Правительства Пензенской области», осуществляется в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 (далее – Постановление № 1119)[12].

2 Сведения о ИС «Веб-сайт Правительства Пензенской области»

ИС «Веб-сайт Правительства Пензенской области» создана в целях повышения уровня открытости исполнительных органов государственной власти Пензенской области, в соответствии с Федеральным законом от 09.02.2009 N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления"[13] (с последующими изменениями), руководствуясь Законом Пензенской области от 22.12.2005 N 906-ЗПО "О Правительстве Пензенской области"[14] (с последующими изменениями) и предназначена для:

- содействия обеспечению реализации прав граждан (физических лиц) и организаций на доступ к информации о деятельности государственных органов;

- создания дополнительных условий и сервисов для взаимодействия Правительства Пензенской области с физическими лицами, юридическими лицами, органами государственной власти и органами местного самоуправления муниципальных образований Пензенской области;

— формирования единого информационного ресурса, содержащего достоверную информацию о деятельности Губернатора Пензенской области и Правительства Пензенской области;

— совершенствования процедур предоставления государственных услуг в электронном виде, повышение их качества и доступности.

Создание ИС «Веб-сайт Правительства Пензенской области» проводилось в соответствии со следующими федеральными законами(далее - ФЗ):

— ФЗ от 09.02.2009 N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления" (с последующими изменениями)[13]

— ФЗ от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с последующими изменениями)[10].

Сопровождение и администрирование ИС «Веб-сайт Правительства Пензенской области» осуществляется сотрудниками органа исполнительной власти, а также организациями осуществляющими сопровождение и разработку программного комплекса ИС «Веб-сайт Правительства Пензенской области» в рамках заключенных государственных контрактов.

ИС «Веб-сайт Правительства Пензенской области» предназначена для:

— содействия обеспечению реализации прав граждан (физических лиц) и организаций на доступ к информации о деятельности государственных органов;

— создания дополнительных условий и сервисов для взаимодействия Правительства Пензенской области с физическими лицами, юридическими лицами, органами государственной власти и органами местного самоуправления муниципальных образований Пензенской области;

— формирования единого информационного ресурса, содержащего достоверную информацию о деятельности Губернатора Пензенской области и Правительства Пензенской области;

— совершенствования процедур предоставления государственных услуг в электронном виде, повышение их качества и доступности.

ИС «Веб-сайт Правительства Пензенской области» является двухуровневой (клиент-серверной), в состав ИС «Веб-сайт Правительства Пензенской области» входят следующие сегменты:

— серверный сегмент ИС «Веб-сайт Правительства Пензенской области» представляет собой сервер агрегации данных и рабочих мест администраторов ИС «Веб-сайт Правительства Пензенской области» размещённых в пределах здания органа исполнительной власти Правительства Пензенской области, находящегося по адресу г.Пенза ул.Московская 75;

— пользовательские сегменты ИС «Веб-сайт Правительства Пензенской области» включающие в себя любые АРМ клиентов, подключенные к сети интернет.

3 Определение класса защищенности ИС «Веб-сайт Правительства Пензенской области»

Информационная система «Веб-сайт Правительства Пензенской области» имеет объектовый масштаб, так как она функционирует на объектах одного органа исполнительной власти и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

В соответствии с Приказом ФСТЭК № 17[7], уровень значимости информации определяется степенью возможного ущерба для обладателя информации и (или) оператора от нарушения конфиденциальности, целостности и доступности. В ИС «Веб-сайт Правительства Пензенской области» осуществляется обработка информации следующих видов: персональные данные и служебная информация. К служебной информации,

обрабатываемой в ИС «Веб-сайт Правительства Пензенской области», относится информация о действиях Правительства Пензенской области, информация необходимая работникам для администрирования ИС, ответы на обращения граждан и другая информация, не отнесенная к категории общедоступной или конфиденциальной.

Уровень значимости информации (УЗ), зависит от степени возможного ущерба от нарушения свойств, безопасности информации и определяется отдельно для каждого вида информации, согласно таблице Б.1.

Таблица Б.1 — Определение уровня значимости информации

Вид информации	Степень возможного ущерба от нарушения свойств безопасности информации			Уровень значимости
	Конфиденциальность	Целостность	Доступность	
персональные данные	Средняя	Средняя	Низкая	УЗ2
служебная информация	Низкая	Средняя	Средняя	УЗ2

Итоговый уровень значимости информации обрабатываемой в ИС «Веб-сайт Правительства Пензенской области», устанавливается по наивысшим признакам степени возможного ущерба, определённым для конфиденциальности, целостности, доступности каждого вида информации. Для ИС «Веб-сайт Правительства Пензенской области» установлен второй уровень значимости информации (УЗ2).

На основании рассмотренных данных, в соответствии с Приказом ФСТЭК № 17[7] в ИС «Веб-сайт Правительства Пензенской области» установлен второй класс (К2) защищенности информационной системы.

Результаты классификации сегментов ИС «Веб-сайт Правительства Пензенской области» должны быть согласованы с _____.

Приложение В
(обязательное)

Модель нарушителя

УТВЕРЖДАЮ

« _ » _____ 2019 г.

ТИПЫ И ВИДЫ НАРУШИТЕЛЕЙ, ИХ ВОЗМОЖНЫЙ ПОТЕНЦИАЛ
(МОДЕЛЬ НАРУШИТЕЛЯ)

1 Общие положения

Модель описывает потенциального нарушителя безопасности и подходы по определению актуальности угроз с учетом возможностей нарушителя и особенностей конкретной ИС. Настоящая Модель разработана в соответствии с требованиями Федерального законодательства и федеральных органов по защите государственных информационных систем.

2 Назначение ИС

Информационная система "Веб-сайт Правительства, Пензенской области" предназначена для:

- содействие обеспечению реализации прав граждан (физических лиц) и организаций на доступ к информации о деятельности государственных органов;
- создание дополнительных условий и сервисов для взаимодействия Правительства Пензенской области с физическими лицами, юридическими лицами, органами государственной власти и органами местного самоуправления муниципальных образований Пензенской области;
- формирование единого информационного ресурса, содержащего достоверную информацию о деятельности Губернатора Пензенской области и Правительства Пензенской области;
- совершенствование процедур предоставления государственных услуг в электронном виде, повышение их качества и доступности.

3 Исходные данные об ИС

Структура информационной системы: Информационная система состоящая из 1 сервера, подключенного к сети интернет при помощи национального провайдера цифровых сервисов ПАО «Ростелеком».

Цели обработки ПДН: обеспечение реализации прав граждан по получению государственных и муниципальных услуг в электронном виде

Тип обрабатываемых ПДН: общедоступные и иные персональные данные

Количество обрабатываемых ПДН: более чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.

Наличие подключений ИС к сетям связи общего пользования и (или) сетям международного информационного обмена: ИС имеет односторонний выход в сеть Интернет.

Режим обработки персональных данных: Многопользовательская система

Режим разграничения прав доступа пользователей информационной системы: ИС с разграничением прав доступа.

Местонахождение технических средств информационной системы: В пределах РФ: – на мощностях интернет-провайдера ПАО «Ростелеком», а также 440025, г.Пенза, ул.Московская, д.75

4 Описание структурно-функциональных характеристик

Возможные способы реализации угроз зависят от структурно-функциональных характеристик и особенностей информационной системы. Поэтому производится анализ характеристик системы и адаптация рассматриваемого перечня угроз. Из числа рассматриваемых угроз исключаются угрозы, для которых отсутствует сценарий реализации.

Инфологическая схема работы системы представлена на рисунке 1.

В таблице В.1 приведено описание информационных потоков, отражённых на рисунке В.1.

Таблица В.1 — Описание информационных потоков

№ Информационного потока	Описание потока
1	Авторизация при помощи ЕСИА, взаимодействие с порталом государственных услуг
2	Авторизация при помощи сервиса Вконтакте
3	Авторизация при помощи сервиса Facebook
4	Авторизация при помощи сервиса Одноклассники
5	Взаимодействие с порталом kremlin.ru
6	Взаимодействие с региональным порталом государственных услуг
7	Передача обращений граждан в систему электронного документооборота, а также получение ответа на обращении

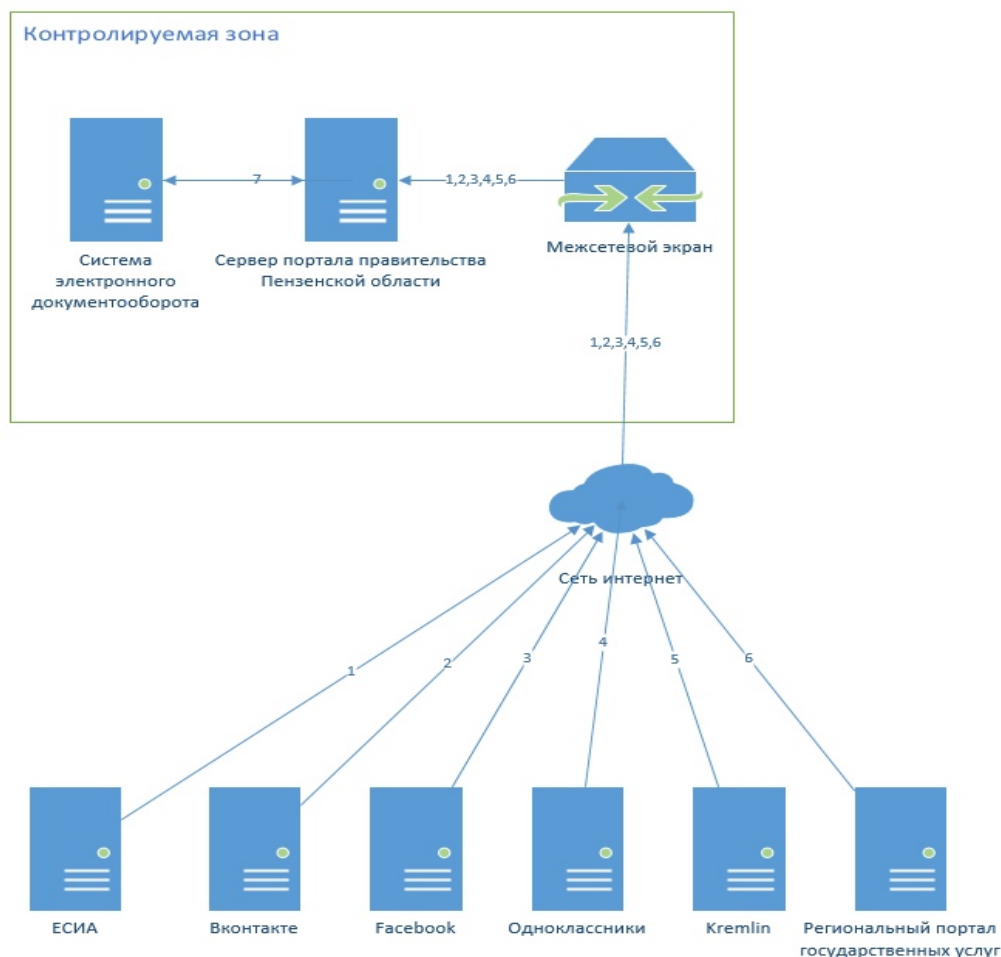


Рисунок В.1 — Инфологическая схема информационной системы

Основываясь на описании информационной системы и особенностей её функционирования, полученных ранее была сформирована модель нарушителя.

Антропогенными источниками угроз являются нарушители. Потенциальные нарушители характеризуются типом и потенциалом. Тип нарушителя может быть внешним или внутренним.

Тип нарушителя зависит от наличия у него доступа к информационной системе и в контролируемую зону. Внешние нарушители не имеют права доступа к информационной системе и реализуют угрозы из-за границ контролируемой зоны. Внутренние нарушители имеют право постоянного или разового доступа в контролируемую зону.

Потенциал нарушителя характеризует уровень его компетентности, наличия ресурсов и мотивации. Потенциал может быть низким, средним или высоким. Описание нарушителей, их возможной мотивации и предполагаемых возможностей приведено в таблице В.2.

Таблица В.2 — Описание нарушителей, их возможной мотивации и предполагаемых возможностей

Нарушители	Категория нарушителей	Потенциал нарушителя	Возможная мотивация	Предполагаемые возможности
Лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора	Внутренний	С низким потенциалом	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему

Продолжение таблицы В.2

Нарушители	Категория нарушителей	Потенциал нарушителей	Возможная мотивация	Предполагаемые возможности
Пользователи информационной системы	Внешний	С низким потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
Бывшие работники	Внешний	С низким потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
Лица, привлекаемые для установки, наладки, монтажа, пуска наладочных и иных работ	Внешний	С низким потенциалом	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему

Продолжение таблицы В.2

Нарушители	Категория нарушителей	Потенциал нарушителей	Возможная мотивация	Предполагаемые возможности
Террористические, экстремистские группировки	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы
Разработчики, производители, поставщики и программных, технических и программнотехнических средств	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или некомпетентные действия	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Продолжение таблицы В.2

Нарушители	Категория нарушителей	Потенциал нарушителей	Возможная мотивация	Предполагаемые возможности
Администраторы информационной системы и администраторы безопасности	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы
Преступные группы (криминальные структуры)	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Продолжение таблицы В.2

Нарушители	Категория нарушителей	Потенциал нарушителя	Возможная мотивация	Предполагаемые возможности
Специальные службы иностранных государств (блоков государств)	Внешний, внутренний	Нарушители с высоким потенциалом	Дискредитация или дестабилизация деятельности органов государственной власти, нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики.	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений

Для рассматриваемой информационной системы отсутствуют следующие нарушители:

— конкурирующие организации, так как в данной сфере конкуренции не существует;

— внешние субъекты, так как в рассматриваемой системе по определению все внешние субъекты взаимодействующие с системой являются пользователями.

6 Ответственные лица

Модель нарушителя подлежит обязательной актуализации по прошествии каждого года, а также при изменении функционала информационной системы.

Ответственным за актуализацию модели нарушителя ИС «Веб-сайт Правительства Пензенской области» назначается _____.

« _ » ____ 2019 г. _____

« _ » ____ 2019 г. _____

Приложение Г
(обязательное)

Модель угроз

УТВЕРЖДАЮ

« _ » _____ 2019 г.

МОДЕЛЬ УГРОЗ

1 Описание информационной системы и особенностей её функционирования.

1.1 Назначение ИС

Информационная система "Веб-сайт Правительства, Пензенской области" предназначена для:

- содействие обеспечению реализации прав граждан (физических лиц) и организаций на доступ к информации о деятельности государственных органов;
- создание дополнительных условий и сервисов для взаимодействия Правительства Пензенской области с физическими лицами, юридическими лицами, органами государственной власти и органами местного самоуправления муниципальных образований Пензенской области;
- формирование единого информационного ресурса, содержащего достоверную информацию о деятельности Губернатора Пензенской области и Правительства Пензенской области;
- совершенствование процедур предоставления государственных услуг в электронном виде, повышение их качества и доступности.

1.2 Исходные данные об ИС

Структура информационной системы: Информационная система состоящая из 1 сервера, подключенного к сети интернет при помощи национального провайдера цифровых сервисов ПАО «Ростелеком».

Цели обработки ПДН: обеспечение реализации прав граждан по получению государственных и муниципальных услуг в электронном виде

Тип обрабатываемых ПДН: общедоступные и иные персональные данные

Количество обрабатываемых ПДН: более чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.

Наличие подключений ИС к сетям связи общего пользования и (или) сетям международного информационного обмена: ИС имеет односторонний выход в сеть Интернет.

Режим обработки персональных данных: Многопользовательская система

Режим разграничения прав доступа пользователей информационной системы: ИС с разграничением прав доступа.

Местонахождение технических средств информационной системы: В пределах РФ: – на мощностях интернет-провайдера ПАО «Ростелеком», а также 440025, г.Пенза, ул.Московская, д.75

1.3 Описание структурно-функциональных характеристик

Возможные способы реализации угроз зависят от структурно-функциональных характеристик и особенностей информационной системы. Поэтому производится анализ характеристик системы и адаптация рассматриваемого перечня угроз. Из числа рассматриваемых угроз исключаются угрозы, для которых отсутствует сценарий реализации.

Инфологическая схема работы системы представлена на рисунке Г.1.

В таблице Г.1 приведено описание информационных потоков, отражённых на рисунке Г.1.

Таблица Г.1 — Описание информационных потоков

№ Информационного потока	Описание потока
1	Авторизация при помощи ЕСИА, взаимодействие с порталом государственных услуг
2	Авторизация при помощи сервиса Вконтакте
3	Авторизация при помощи сервиса Facebook
4	Авторизация при помощи сервиса Одноклассники

Продолжение таблицы Г.1

№ Информационного потока	Описание потока
5	Взаимодействие с порталом kremlin.ru
6	Взаимодействие с региональным порталом государственных услуг
7	Передача обращений граждан в систему электронного документооборота, а также получение ответа на обращения

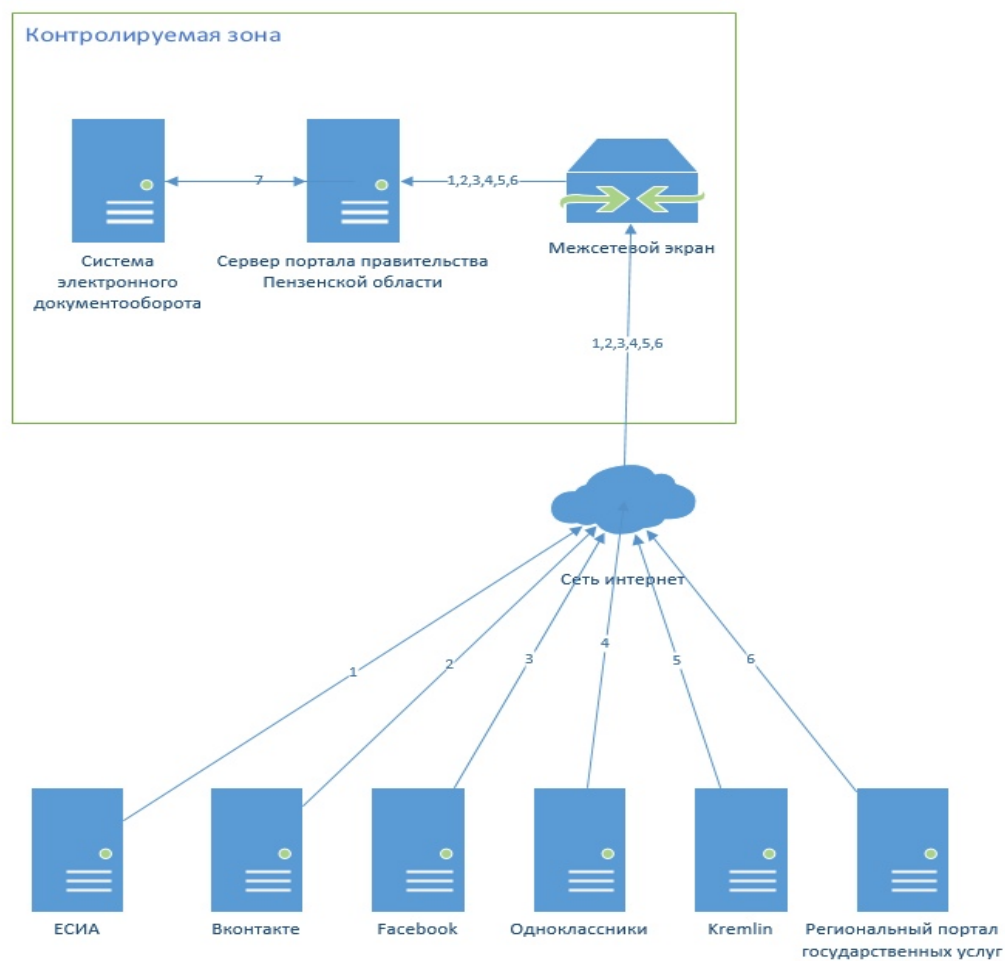


Рисунок Г.1 — Инфологическая схема информационной системы

2 Типы и виды нарушителей, их возможный потенциал (модель нарушителя)

Основываясь на описании информационной системы и особенностей её функционирования, полученных ранее была сформирована модель нарушителя.

Антропогенными источниками угроз являются нарушители. Потенциальные нарушители характеризуются типом и потенциалом. Тип нарушителя может быть внешним или внутренним.

Тип нарушителя зависит от наличия у него доступа к информационной системе и в контролируемую зону. Внешние нарушители не имеют права доступа к информационной системе и реализуют угрозы из-за границ контролируемой зоны. Внутренние нарушители имеют право постоянного или разового доступа в контролируемую зону.

Потенциал нарушителя характеризует уровень его компетентности, наличия ресурсов и мотивации. Потенциал может быть низким, средним или высоким. Описание нарушителей, их возможной мотивации и предполагаемых возможностей приведено в таблице Г.2.

Таблица Г.2 — Описание нарушителей, их возможной мотивации и предполагаемых возможностей

Нарушители	Категория нарушителей	Потенциал нарушителя	Возможная мотивация	Предполагаемые возможности
Лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора	Внутренний	С низким потенциалом	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему

Продолжение таблицы Г.2

Нарушители	Категория нарушителей	Потенциал нарушителей	Возможная мотивация	Предполагаемые возможности
Пользователи информационной системы	Внешний	С низким потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
Бывшие работники	Внешний	С низким потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
Лица, привлекаемые для установки, наладки, монтажа, пуска наладочных и иных работ	Внешний	С низким потенциалом	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему

Продолжение таблицы Г.2

Нарушители	Категория нарушителей	Потенциал нарушителей	Возможная мотивация	Предполагаемые возможности
Террористические, экстремистские группировки	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы
Разработчики, производители, поставщики и программных, технических и программнотехнических средств	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или некомпетентные действия	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Продолжение таблицы Г.2

Нарушители	Категория нарушителей	Потенциал нарушителей	Возможная мотивация	Предполагаемые возможности
Администраторы информационной системы и администраторы безопасности	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы
Преступные группы (криминальные структуры)	Внешний	Нарушители с базовым повышенным (средним) потенциалом	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Продолжение таблицы Г.2

Нарушители	Категория нарушителей	Потенциал нарушителя	Возможная мотивация	Предполагаемые возможности
Специальные службы иностранных государств (блоков государств)	Внешний, внутренний	Нарушители с высоким потенциалом	Дискредитация или дестабилизация деятельности органов государственной власти, нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики.	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений

Для рассматриваемой информационной системы отсутствуют следующие нарушители:

— конкурирующие организации, так как в данной сфере конкуренции не существует;

— внешние субъекты, так как в рассматриваемой системе по определению все внешние субъекты взаимодействующие с системой являются пользователями.

3 Определение актуальных угроз

3.1 Определение уровня исходной защищённости

Для оценки возможности реализации угрозы применяются два показателя:

- уровень исходной защищённости ИС;
- частота (вероятность) реализации рассматриваемой угрозы.

В ходе эксплуатации информационной системы уровень ее защищенности (Y1) определяется следующим образом:

а) в информационной системе обеспечивается высокий уровень защищенности (Y1), если в ходе эксплуатации информационной системы не появились дополнительные угрозы безопасности информации или в отношении появившихся дополнительных угроз безопасности информации с высокой оперативностью («за минуты») могут быть приняты меры защиты информации, нейтрализующие эти угрозы;

б) в информационной системе обеспечивается средний уровень защищенности (Y1), если в ходе эксплуатации информационной системы появились дополнительные угрозы безопасности информации и в отношении них оперативно («за часы») могут быть приняты меры защиты информации, нейтрализующие эти угрозы;

в) в информационной системе обеспечивается низкий уровень защищенности (Y1), если в ходе эксплуатации информационной системы появились дополнительные угрозы безопасности информации и в отношении них не могут быть с высокой оперативностью или оперативно приняты меры защиты информации, нейтрализующие эти угрозы.

В ходе эксплуатации системы в течение нескольких лет, возникали дополнительные угрозы безопасности информации, в отношении которых были приняты меры по их нейтрализации в течение нескольких часов.

Таким образом, можно сделать вывод, что информационная система имеет средний уровень исходной защищённости.

Возможность реализации j -ой угрозы безопасности информации (Y_j) в зависимости от уровня защищенности информационной системы ($Y_{1П}$) и потенциала нарушителя (Y_2) определяется как высокая, средняя или низкая в соответствии с таблицей Г.3.

Таблица Г.3 — Возможность реализации угрозы безопасности информации

Уровень защищённости	Высокий	Средний	Низкий
Потенциал нарушителя			
Базовый(низкий)	Низкая	Средняя	Высокая
Базовый повышенный(средний)	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

3.2 Оценка степени возможного ущерба от реализации угрозы безопасности информации

Для оценки степени возможного ущерба от реализации угрозы безопасности информации определяются возможный результат реализации угрозы безопасности информации в информационной системе, вид ущерба, к которому может привести реализация угрозы безопасности информации, степень последствий от реализации угрозы безопасности информации для каждого вида ущерба.

В качестве результата реализации угрозы безопасности информации рассматриваются непосредственное или опосредованное воздействие на конфиденциальность, целостность, доступность информации, содержащейся в информационной системе.

Результат реализации угрозы безопасности информации определяется воздействием угрозы на каждое свойство безопасности информации (конфиденциальность, целостность, доступность) в отдельности в соответствии

с таблицей Г.4. При обработке в информационной системе двух и более видов информации (служебная тайна, персональные данные, налоговая тайна, иные установленные законодательством Российской Федерации виды информации) воздействие на конфиденциальность, целостность, доступность определяется отдельно для каждого вида информации, содержащейся в информационной системе.

Таблица Г.4 - Результат реализации угрозы безопасности информации

Свойство безопасности информации	Результат реализации угрозы безопасности информации	
	Не оказывает воздействия	Оказывает воздействие
Конфиденциальность Хк	В результате реализации угрозы безопасности информации отсутствует возможность неправомерного доступа, копирования, предоставления или распространения информации	В результате реализации угрозы безопасности информации возможны неправомерный доступ, копирование, предоставление или распространение информации
Целостность Хц	В результате реализации угрозы безопасности информации отсутствует возможность уничтожения или модифицирования информации	В результате реализации угрозы безопасности информации возможно уничтожение или модифицирование информации
Доступность Хд	В результате реализации угрозы безопасности информации отсутствует возможность блокирования информации	В результате реализации угрозы безопасности информации возможно блокирование информации

Основные виды ущерба и возможные негативные последствия, к которым может привести нарушение конфиденциальности, целостности, доступности информации, приведены в таблице Г.5.

Таблица Г.5 — Вид ущерба и возможные негативные последствия

Вид ущерба	Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации
Экономический (финансовый)	<p>Снижение, как минимум, одного экономического показателя.</p> <p>Потеря (кража) финансовых средств.</p> <p>Недополучение ожидаемой (прогнозируемой) прибыли.</p> <p>Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.</p> <p>Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).</p>

Продолжение таблицы Г.5

Вид ущерба	Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации
Экономический (финансовый)	<p>Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.</p> <p>Потеря клиентов, поставщиков.</p> <p>Потеря конкурентного преимущества.</p> <p>Невозможность заключения договоров, соглашений.</p> <p>Другие прямые или косвенные финансовые потери</p>
Социальный	<p>Создание предпосылок для нанесения вреда здоровью граждан.</p> <p>Возможность нарушения функционирования объектов обеспечения жизнедеятельности граждан.</p> <p>Организация пикетов, забастовок, митингов и других акций.</p> <p>Увольнения.</p> <p>Увеличение количества жалоб в органы государственной власти или органы местного самоуправления.</p> <p>Появление негативных публикаций в общедоступных источниках.</p> <p>Невозможность (прерывание) предоставления социальных услуг (сервисов).</p> <p>Другие последствия, приводящие к нарастанию социальной напряженности в обществе</p>
Политический	<p>Создание предпосылок к обострению отношений в международных отношениях.</p> <p>Срыв двусторонних (многосторонних) контактов с зарубежными партнерами.</p> <p>Неспособность выполнения международных (двусторонних) договорных обязательств.</p> <p>Невозможность заключения международных (двусторонних) договоров, соглашений.</p> <p>Создание предпосылок к внутривнутриполитическому кризису.</p> <p>Нарушение выборного процесса.</p> <p>Другие последствия во внутривнутриполитической и внешнеполитической областях деятельности</p>
Репутационный	<p>Нарушение законодательных и подзаконных актов. Нарушение деловой репутации.</p> <p>Снижение престижа.</p> <p>Дискредитация работников.</p> <p>Утрата доверия.</p> <p>Неспособность выполнения договорных обязательств.</p> <p>Другие последствия, приводящие к нарушению репутации</p>
Ущерб в области обороны, безопасности и правопорядка	<p>Создание предпосылок к наступлению негативных последствий для обороны, безопасности и правопорядка.</p> <p>Нарушение общественного правопорядка.</p> <p>Неблагоприятное влияние на обеспечение общественного правопорядка.</p> <p>Возможность потери или снижения уровня контроля за общественным правопорядком.</p> <p>Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации.</p> <p>Другие последствия, приводящие к ущербу в области обороны, безопасности и правопорядка</p>

Продолжение таблицы Г.5

Вид ущерба	Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации
Ущерб субъекту персональных данных	Создание угрозы личной безопасности. Финансовые или иные материальные потери физического лица. Вторжение в частную жизнь. Создание угрозы здоровью. Моральный вред. Утрата репутации. Другие последствия, приводящие к нарушению прав субъекта персональных данных
Технологический	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Принятие неправильных решений. Простой информационной системы или сегмента информационной системы. Другие последствия, приводящие к нарушению технологии обработки информации

Степень возможного ущерба определяется экспертным методом в соответствии с таблицей Г.6.

Таблица Г.6 — Степень возможного ущерба

Степень ущерба	Характеристика степени ущерба
Высокая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
Средняя	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
Низкая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств

При обработке в информационной системе двух и более видов информации (служебная тайна, персональные данные, налоговая тайна и иные установленные законодательством Российской Федерации виды информации)

степень возможного ущерба определяется отдельно для каждого вида информации, обрабатываемой в информационной системе, применительно к каждому виду ущерба. Итоговая степень возможного ущерба устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации применительно к каждому виду ущерба.

3.3 Определение актуальности угрозы безопасности информации

Актуальной считается угроза, которая может быть реализована в ИС и представляет опасность для неё. Для определения актуальности конкретной угрозы безопасности ИС определяются:

- возможность реализации угрозы;
- опасность угрозы.

Решение об актуальности угрозы безопасности информации для информационной системы с заданными структурно-функциональными характеристиками и условиями функционирования принимается в соответствии с таблицей Г.7.

Таблица Г.7 — Финальная оценка актуальности угрозы

Вероятность (возможность) реализации угрозы	Степень возможного ущерба		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

Расчёт коэффициентов реализуемости для угроз из банка угроз ФСТЭК[9] для ИС, а также отнесение угроз к актуальным согласно правил, приведенных в таблице Г.7, приведено в таблице Г.8.

Таблица Г.8 — Расчёт коэффициентов реализуемости для каждой угрозы в ИС и определение актуальных угроз

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
1	Угроза автоматического распространения вредоносного кода в грид-системе	Угроза заключается в возможности внедрения и запуска вредоносного кода от имени доверенного процесса на любом из ресурсных центров грид-системы и его автоматического распространения на все узлы грид-системы. Данная угроза обусловлена слабостями технологии грид-вычислений – высоким уровнем автоматизации при малой администрируемости грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий легального пользователя грид-системы	С						Данная технология не применяется в ИС
2	Угроза агрегирования данных, передаваемых в грид-системе	Угроза заключается в возможности раскрытия нарушителем защищаемой информации путём выявления задействованных в её обработке узлов, сбора, анализа и обобщения данных, перехватываемых в сети передачи данных грид-системы. Данная угроза обусловлена слабостью технологии грид-вычислений – использованием незащищённых каналов сети Интернет как транспортной сети грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя: сил и средств, достаточных для компенсации чрезвычайной распределённости грид-заданий между узлами грид-системы; привилегий, достаточных для перехвата трафика сети передачи данных между элементами (узлами) грид-системы/	С						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
3	Угроза анализа криптографических алгоритмов и их реализации	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	С	ПДН	К	Социальный;	В	Актуальная	
						Репутационный;	В		
						Ущерб субъекту ПДН	В		
				СТ	К	Репутационный;	С		
						Социальный	С		
4	Угроза аппаратного сброса пароля BIOS	Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера	Н	ПДН	Ц	Технологический	Н	Неактуальная	
				СТ	Ц	Технологический	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
5	Угроза внедрения вредоносного кода в BIOS	Угроза заключается в возможности заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения BIOS/UEFI на версию, уже содержащую вредоносный код. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI и заменой чипсета BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера	В	ПДН	К	Ущерб субъекту ПДН	В	Актуальная	
					Ц	Технологический	С		
					Д	Репутационный	В		
				СТ	К	Социальный	С		
					Ц	Технологический	С		
					Д	Технологический	С		
6	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).	Н	ПДН	К	Ущерб субъекту ПДН	В	Актуальная	
					Ц	Технологический	Н		
					Д	Репутационный	С		
				СТ	К	Социальный	С		
					Ц	Репутационный	С		
					Д	Политический; Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
6		Реализация данной угрозы возможна: в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников; при наличии у него привилегий установки программного обеспечения; в случае неизменных владельцем учетных данных IoT-устройства (заводских пароля и логина)							
7	Угроза воздействия на программы с высокими привилегиями	Угроза заключается в возможности повышения нарушителем своих привилегий в дискредитированной системе (получения привилегии дискредитированных программ) путём использования ошибок в программах и выполнения произвольного кода с их привилегиями. Данная угроза обусловлена слабостями механизма проверки входных данных и команд, а также мер по разграничению доступа. Реализация данной угрозы возможна при условиях: обладания дискредитируемой программой повышенными привилегиями в системе; осуществления дискредитируемой программой приёма входных данных от других программ или от пользователя; нарушитель имеет возможность осуществлять передачу данных к дискредитируемой программе	С	ПДН	К	Ущерб субъекту ПДН	С	Актуальная	
					Ц	Репутационный	С		
				СТ	К	Политический	С		
					Ц	Экономический	С		
8	Угроза восстановления аутентификационной информации	Угроза заключается в возможности подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе. Данная угроза обусловлена значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой, что определяет два следствия: время подбора в основном определяется не объёмом аутентификационной информации, а объёмом данных её хеш-кода; восстановленная аутентификационная информация может не совпадать	Н	ПДН	К	Ущерб субъекту ПДН	Н	Неактуальная	
				СТ	К	Репутационный	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
8		с исходной (при применении некоторых алгоритмов для нескольких наборов исходных данных могут быть получены одинаковые результаты – хеш-коды). Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную»							
9	Угроза восстановления предыдущей уязвимой версии BIOS	Угроза заключается в возможности осуществления вынужденного перехода на использование BIOS/UEFI, содержащей уязвимости. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. При использовании технологии обновления BIOS/UEFI возможно возникновение следующей ситуации (условия, характеризующие ситуацию указаны в хронологическом порядке): на компьютере установлена некоторая версия BIOS/UEFI, для которой на момент её работы не известны уязвимости; в силу некоторых обстоятельств BIOS/UEFI проходит процедуру обновления, сохраняя при этом предыдущую версию BIOS/UEFI на случай «отката» системы; публикуются данные о существовании уязвимостей в предыдущей версии BIOS/UEFI; происходит сбой в работе системы, в результате чего текущая (новая) версия BIOS/UEFI становится неработоспособной (например, нарушается её целостность); пользователь осуществляет штатную процедуру восстановления работоспособности системы – проводит «откат» системы к предыдущему работоспособному состоянию	Н	ПДН	К	Ущерб субъекту ПДН	Н	Неактуальная	
					Ц	Технологический	Н		
					Д	Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический	Н		
					Д	Технологический Репутационный	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
10	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 выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора	С	ПДН	К	Ущерб субъекту ПДН	В	Актуальная	
					Ц	Технологический	Н		
					Д	Технологический	Н		
				СТ	К	Социальный	С		
					Ц	Технологический	В		
					Д	Репутационный	С		
11	Угроза деавторизации санкционированного клиента беспроводной сети	Угроза заключается в возможности автоматического разрыва соединения беспроводной точки доступа с санкционированным клиентом беспроводной сети. Данная угроза обусловлена слабостью технологий сетевого взаимодействия по беспроводным каналам передачи данных – сведения о MAC-адресах беспроводных клиентов доступны всем участникам сетевого взаимодействия. Реализация данной угрозы возможна при условии подключения нарушителем к беспроводной сети устройства, MAC-адрес которого будет полностью совпадать с MAC-адресом дискредитируемого санкционированного клиента	Н	ПДН	Д	Репутационный	С	Актуальная	
				СТ	Д	Репутационный	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
12	Угроза деструктивн ого изменения конфигурац ии/среды окружения программ	Угроза заключается в возможности деструктивного программного воздействия на дискредитируемое приложение путём осуществления манипуляций с используемыми им конфигурационными файлами или библиотеками. Данная угроза обусловлена слабостями мер контроля целостности конфигурационных файлов или библиотек, используемых приложениями. Реализация данной угрозы возможна в случае наличия у нарушителя прав осуществления записи в файловые объекты, связанные с конфигурацией/средой окружения программы, или возможности перенаправления запросов дискредитируемой программы от защищённых файловых объектов к ложным	Н	ПДН	К	Ущерб субъекту ПДН	С	Акту альна я	
					Ц	Технологический	С		
					Д	Социальный Репутационный	С		
				СТ	К	Репутационный	С		
					Ц	Технологический	С		
					Д	Репутационный	С		
13	Угроза деструктивн ого использован ия декларирова нного функционал а 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	Н	ПДН	Ц	Репутационный	Н	Неакт уальн ая	
				СТ	Ц	Технологический	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
14	Угроза длительного удержания вычислительных ресурсов пользователями	Угроза заключается в возможности ограничения нарушителем доступа конечных пользователей к вычислительному ресурсу за счёт принудительного удержания его в загруженном состоянии путём осуществления им многократного выполнения определённых деструктивных действий или эксплуатации уязвимостей программ, распределяющих вычислительные ресурсы между задачами. Данная угроза обусловлена слабостями механизмов балансировки нагрузки и распределения вычислительных ресурсов. Реализация угрозы возможна в случае, если у нарушителя имеется возможность делать запросы, которые в совокупности требуют больше времени на выполнение, чем запросы пользователя	Н	ПДН	Д	Репутационный	С	Акту альна я	
				СТ	Д	Технологический	С		
15	Угроза доступа к защищаемым файлам с использованием обходного пути	Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы. Реализация данной угрозы возможна при условиях: наличие у нарушителя прав доступа к некоторым объектам файловой системы; отсутствие проверки вводимых пользователем данных; наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с её помощью	Н	ПДН	К	Ущерб субъекту ПДН	С	Акту альна я	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
16	Угроза доступа к локальным файлам сервера при помощи URL	<p>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.</p> <p>Данная угроза обусловлена слабостями механизма проверки вводимых пользователем запросов, который не делает различий между запросами на доступ к файловой системе и URL-запросами.</p> <p>Реализация данной угрозы возможна в случае наличия у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Социальный Репутационный	С		
17	Угроза доступа/перехвата/изменения HTTP cookies	<p>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).</p> <p>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.</p> <p>Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к cookies-файлам и отсутствии проверки целостности их значений со стороны дискредитируемого приложения</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Д	Репутационный	С		
				СТ	К	Репутационный	С		
					Д	Технологический	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
18	Угроза загрузки нештатной операционной системы	Угроза заключается в возможности подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии доступности нарушителю следующего параметра настройки BIOS/UEFI – указания источника загрузки операционной системы	Н	ПДН	К	Ущерб субъекту ПДН	Н	Неактуальная	
					Ц	Технологический	Н		
					Д	Репутационный	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический	Н		
					Д	Технологический	Н		
19	Угроза заражения DNS-кеша	Угроза заключается в возможности перенаправления нарушителем сетевого трафика через собственный сетевой узел путём опосредованного изменения таблиц соответствия IP- и доменных имён, хранимых в DNS-сервере, за счёт генерации лавины возможных ответов на запрос DNS-сервера легальному пользователю или за счёт эксплуатации уязвимостей DNS-сервера. Данная угроза обусловлена слабостями механизмов проверки подлинности субъектов сетевого взаимодействия, а также уязвимостями DNS-сервера, позволяющими напрямую заменить DNS-кеш DNS-сервера. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий, достаточных для отправки сетевых запросов к DNS-серверу	Н	ПДН	К	Ущерб субъекту ПДН	Н	Неактуальная	
				СТ	К	Репутационный	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
20	Угроза злоупотребл ения возможност ями, предоставле нными потребителя м облачных услуг	Угроза заключается в возможности осуществления потребителем облачных услуг (нарушителем) рассылки спама, несанкционированного доступа к виртуальным машинам других потребителей облачных услуг или осуществления других деструктивных программных воздействий на различные системы с помощью арендованных ресурсов облачного сервера. Данная угроза обусловлена тем, что потребитель облачных услуг может устанавливать собственное программное обеспечение на облачный сервер. Реализация данной угрозы возможна путём установки и запуска потребителем облачных услуг вредоносного программного обеспечения на облачный сервер. Успешная реализация данной угрозы потребителем облачных услуг оказывает негативное влияние на репутацию поставщика облачных услуг	Н	ПДН	К	Репутационный			Данная технология не применяется в ИС
					Ц	Репутационный			
					Д	Репутационный			
				СТ	К	Репутационный			
					Ц	Технологический			
					Д	Технологический			
21	Угроза злоупотребл ения доверием потребителе й 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)	Н	ПДН	К	Репутационный			Данная технология не применяется в ИС
					Ц	Репутационный			
				СТ	К	Репутационный			
					Ц	Технологический			

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
22	Угроза избыточного выделения оперативной памяти	Угроза заключается в возможности выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти, доступных в системе для выделения в ответ на запросы программ легальных пользователей. Данная угроза обусловлена наличием слабостей механизма контроля выделения оперативной памяти различным программам. Реализация данной угрозы возможна при условии нахождения вредоносного программного обеспечения в системе в активном состоянии	Н	ПДН	Д	Технологический	Н	Акту альна я	
				СТ	Д	Технологический	С		
23	Угроза изменения компонентов системы	Угроза заключается в возможности получения нарушителем доступа к сети Интернет (при его отсутствии в системе), к хранимым на личных мобильных устройствах 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	Н	ПДН	Ц	Технологический	С	Акту альна я	
					Д	Социальный	Н		
				СТ	Ц	Технологический	С		
					Д	Технологический	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
24	Угроза изменени я режимов работы аппаратн ых элементов компьюте ра	Угроза заключается в возможности изменения нарушителем режимов работы аппаратных элементов компьютера путём несанкционированного переконфигурирования BIOS/UEFI, что позволяет: за счёт изменения частоты системной шины, режима передачи данных по каналам связи и т.п. повлиять на общую производительность компьютера или вызвать сбои в его работе; за счёт понижения входного напряжения, отключения систем охлаждения временно обеспечить неработоспособность компьютера; за счёт задания недопустимых параметров работы устройств (порогового значения отключения устройства при перегреве, входного напряжения и т.п.) привести к физическому выходу из строя отдельных аппаратных элементов компьютера. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение соответствующих параметров настройки	В	ПДН	Ц	Технологический	В	Акту альна я	
					Д	Технологический	С		
				СТ	Ц	Технологический	В		
					Д	Технологический	С		
25	Угроза изменени я системн ых и глобальн ых переменн ых	Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путём изменения используемых дискредитируемыми программами единых системных и глобальных переменных. Данная угроза обусловлена слабостями механизма контроля доступа к разделяемой памяти, а также уязвимостями программных модулей приложений, реализующих контроль целостности внешних переменных. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к системным и глобальным переменным и отсутствии проверки целостности их значений со стороны дискредитируемого приложения	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Социальный Технологический	С		
					Д	Технологический	С		
				СТ	К	Социальный	С		
					Ц	Технологический	В		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
26	Угроза искажения XML-схемы	Угроза заключается в возможности изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером. Данная угроза обусловлена слабостями мер обеспечения целостности передаваемых при клиент-серверном взаимодействии данных, а также слабостями 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	С	ПДН	Ц	Репутационный Социальный Технологический	В	Акту альна я	
					Д	Репутационный Социальный	С		
				СТ	Ц	Технологический	В		
					Д	Технологический	С		
27	Угроза искажения и выводимой на периферийн ые устройства информации	Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок						Неакту альна я	Не применима к рассматрив аемой системе

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
28	Угроза использования альтернативных путей доступа к ресурсам	<p>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).</p> <p>Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации, слабостями фильтрации входных данных.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя:</p> <p>возможности ввода произвольных данных в адресную строку;</p> <p>сведений о пути к защищаемому ресурсу;</p> <p>возможности изменения интерфейса ввода входных данных</p>	Н	ПДН	К	Репутационный Социальный	С	Актуальная	
				СТ	К	Социальный Репутационный	С		
29	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	<p>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).</p> <p>Данная угроза обусловлена слабостями мер очистки памяти от «процессов-потомков» завершённых заданий, а также процессов, запущенных вредоносным программным обеспечением.</p> <p>Реализация данной угрозы возможна при условии некорректного завершения выполненных задач или наличия вредоносных процессов в памяти суперкомпьютера в активном состоянии</p>						Неактуальная	Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	<p>Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты.</p> <p>Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset).</p> <p>Реализация данной угрозы возможна при одном из следующих условий: наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты; успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты</p>	Внутренний нарушитель с низким потенциалом	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный	Н		
				СТ	К	Ущерб субъекту ПДН Социальный	Н		
					Ц	Технологический	С		
					Д	Технологический	С		
			Внешний нарушитель со средним потенциалом	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С		
					Ц	Репутационный	С		
					Д	Репутационный	Н		
				СТ	К	Ущерб субъекту ПДН Социальный	Н		
					Ц	Технологический	С		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
31	Угроза использования механизмов авторизации для повышения привилегий	Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки. Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе	Н	ПДН	К	Репутационный Социальный Ущерб субъекту ПДН	С	Актуальная	
				СТ	К	Репутационный Ущерб субъекту ПДН	Н		
32	Угроза использования поддельных цифровых подписей BIOS	Угроза заключается в возможности установки уязвимой версии обновления BIOS/UEFI или версии, содержащей вредоносное программное обеспечение, но имеющей цифровую подпись. Данная угроза обусловлена слабостями мер по контролю за благонадёжностью центров выдачи цифровых подписей. Реализация данной угрозы возможна при условии выдачи неблагонадёжным центром сертификации цифровой подписи на версию обновления BIOS/UEFI, содержащую уязвимости, или на версию, содержащую вредоносное программное обеспечение (т.е. при осуществлении таким центром подлога), а также подмены нарушителем доверенного источника обновлений	С	ПДН	Ц	Репутационный Социальный	С	Актуальная	
				СТ	Ц	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
33	Угроза использования слабостей кодирования входных данных	Угроза заключается в возможности осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.). Данная угроза обусловлена слабостями механизма контроля входных данных. Реализация данной угрозы возможна при условиях: дискредитируемая система принимает входные данные от нарушителя; нарушитель обладает возможностью управления одним или несколькими параметрами входных данных	С	ПДН	Ц	Репутационный Социальный Технологический	С	Актуальная	
					Д	Репутационный Технологический	Н		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический	Н		
34	Угроза использования слабостей протоколов сетевого/локального обмена данными	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов. Данная угроза обусловлена слабостями самих протоколов (заложенных в них алгоритмов), ошибками, допущенными в ходе реализации протоколов, или уязвимостями, внедряемыми автоматизированными средствами проектирования/разработки. Реализация данной угрозы возможна в случае наличия слабостей в протоколах сетевого/локального обмена данными	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
35	Угроза использования слабых криптографических алгоритмов BIOS	Угроза заключается в сложности проверки реальных параметров работы и алгоритмов, реализованных в криптографических средствах BIOS/UEFI. При этом доверие к криптографической защите будет ограничено доверием к производителю BIOS. Данная угроза обусловлена сложностью использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI. Возможность реализации данной угрозы снижает достоверность оценки реального уровня защищённости системы	В	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный	С		
				СТ	К	Ущерб субъекту ПДН Социальный	С		
					Ц	Технологический	В		
					Д	Технологический	С		
36	Угроза исследования механизмов работы программы	Угроза заключается в возможности проведения нарушителем обратного инжиниринга кода программы и дальнейшего исследования его структуры, функционала и состава в интересах определения алгоритма работы программы и поиска в ней уязвимостей. Данная угроза обусловлена слабостями механизма защиты кода программы от исследования. Реализация данной угрозы возможна в случаях: наличия у нарушителя доступа к исходным файлам программы; наличия у нарушителя доступа к дистрибутиву программы и отсутствия механизма защиты кода программы от исследования	С	ПДН				Неактуальная	Не применима к рассматриваемой системе
				СТ					

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
37	Угроза исследования приложения через отчёты об ошибках	Угроза заключается в возможности исследования нарушителем алгоритма работы дискредитируемого приложения и его предполагаемой структуры путём анализа генерируемых этим приложением отчётов об ошибках. Данная угроза обусловлена размещением защищаемой информации (или информации, обобщение которой может раскрыть защищаемые сведения о системе) в генерируемых отчётах об ошибках. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Ущерб субъекту ПДН Репутационный	С		
38	Угроза истощения вычислительных ресурсов хранилища больших данных	Угроза заключается в возможности временного возникновения состояния типа «отказ в обслуживании» у хранилища больших данных. Данная угроза обусловлена постоянным трудно контролируемым заполнением занятого дискового пространства за счёт данных, непрерывно поступающих из различных информационных источников, и слабостями технологий доступа и хранения информации в хранилищах больших данных. Реализация данной угрозы возможна при условии мгновенного (текущего) превышения скорости передачи данных над скоростью их сохранения (в силу недостаточности пропускной способности канала связи или скорости выделения свободного пространства и сохранения на него поступающих данных) или при условии временного отсутствия свободного места в хранилище (в силу некорректного управления хранилищем или в результате осуществления нарушителем деструктивного программного воздействия на механизм контроля за заполнением хранилища путём изменения параметров или логики его работы)	Н	ПДН				Не актуальная	Данная технология не применяется в ИС
				СТ					

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Угроза заключается в возможности нарушения (невозможности осуществления) процедуры обновления BIOS/UEFI при исчерпании запаса необходимых для её проведения ключей. Данная угроза обусловлена ограниченностью набора ключей, необходимых для обновления BIOS/UEFI. Реализация данной угрозы возможна путём эксплуатации уязвимостей средств обновления набора ключей, или путём использования нарушителем программных средств перебора ключей	С	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
				СТ	Ц	Репутационный Технологический	С		
40	Угроза конфликта юрисдикций различных стран	Угроза заключается в возможности отказа в трансграничной передаче защищаемой информации в рамках оказания облачных услуг в соответствии с требованиями локального законодательства стран, резиденты которых участвуют в оказании облачных услуг. Данная угроза обусловлена тем, что в зависимости от особенностей законодательства различных стран, резиденты которых участвуют в оказании облачных услуг, при обеспечении информационной безопасности могут использоваться правовые меры различных юрисдикций. 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	Н	ПДН				Не актуа льная	Не применима к рассматрив аемой системе
				СТ					

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
41	Угроза межсайтового скриптинга	Угроза заключается в возможности внедрения нарушителем участков вредоносного кода на сайт дискредитируемой системы таким образом, что он будет выполнен на рабочей станции просматривающего этот сайт пользователя. Данная угроза обусловлена слабостями механизма проверки безопасности при обработке запросов и данных, поступающих от веб-сайта. Реализация угрозы возможна в случае, если клиентское программное обеспечение поддерживает выполнение сценариев, а нарушитель имеет возможность отправки запросов и данных в дискредитируемую систему	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Технологический Социальный	В	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Технологический Социальный	С		
					Ц	Технологический	В		
					Д	Технологический	С		
42	Угроза межсайтовой подделки запроса	Угроза заключается в возможности отправки нарушителем дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс, при переходе на который автоматически будут выполнены неправомерные вредоносные действия от имени дискредитированного пользователя. Данная угроза обусловлена уязвимостями браузеров, которые позволяют выполнять действия без подтверждения или аутентификации со стороны дискредитируемого пользователя. Реализация угрозы возможна в случае, если дискредитируемый пользователь сохраняет аутентификационную информацию с помощью браузера	С	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический	С		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обраба тываем ой инфор мации	Нарушаемы е свойства безопаснос ти информаци и	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
43	Угроза нарушения доступности облачного сервера	Угроза заключается в возможности прекращения оказания облачных услуг всем потребителям (или группе потребителей) из-за нарушения доступности для них облачной инфраструктуры. Данная угроза обусловлена тем, что обеспечение доступности не является специфичным требованием безопасности информации для облачных технологий, и, кроме того, облачные системы реализованы в соответствии с сервис-ориентированным подходом. Реализация данной угрозы возможна при переходе одного или нескольких облачных серверов в состояние «отказ в обслуживании». Более того, способность динамически изменять объём предоставляемых потребителям облачных услуг может быть использована нарушителем для реализации угрозы. При этом успешно реализованная угроза в отношении всего лишь одного облачного сервиса позволит нарушить доступность всей облачной системы	Н	ПДН	Д			Не актуальная	Данная технология не применяется в ИС
				СТ	Д				
44	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Угроза заключается в возможности нарушения безопасности пользовательских данных программ, функционирующих внутри виртуальной машины, вредоносным программным обеспечением, функционирующим вне виртуальной машины. Данная угроза обусловлена наличием уязвимостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри виртуальной машины, от несанкционированного доступа со стороны вредоносного программного обеспечения, функционирующего вне виртуальной машины. Реализация данной угрозы возможна при условии успешного преодоления вредоносным программным кодом границ виртуальной машины не только за счёт эксплуатации уязвимостей гипервизора, но и путём осуществления такого воздействия с более низких (по отношению к гипервизору) уровней функционирования системы	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический	С		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
45	Угроза нарушения изоляции среды исполнения BIOS	Угроза заключается в возможности изменения параметров и (или) логики работы программного обеспечения BIOS/UEFI путём программного воздействия из операционной системы компьютера или путём несанкционированного доступа к каналу сетевого взаимодействия серверного сервис-процессора. Данная угроза обусловлена слабостями технологий разграничения доступа к BIOS/UEFI, его функциям администрирования и обновления, со стороны операционной системы или каналов связи. Реализация данной угрозы возможна: со стороны операционной системы – при условии наличия BIOS/UEFI функционала обновления и (или) управления программным обеспечением BIOS/UEFI из операционной системы; со стороны сети – при условии наличия у дискредитируемого серверного сервис-процессора достаточных привилегий для управления всей системой, включая модификацию BIOS/UEFI серверов системы, и дискредитируемого сервера	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный	Н		
					Д	Репутационный	Н		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
46	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия. Данная угроза обусловлена наличием множества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между её уровнями. Реализация данной угрозы возможна в случае возникновения ошибок при проведении аутентификации субъектов виртуального информационного взаимодействия	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Д	Репутационный	Н		
				СТ	К	Репутационный Социальный	Н		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
47	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Угроза заключается в возможности значительного снижения производительности грид-системы, вплоть до временного нарушения её работоспособности при появлении нетипичной сетевой нагрузки (в т.ч. вызванной распределённой DoS-атакой, активностью других пользователей в сети и др.). Данная угроза обусловлена слабостью технологий грид-вычислений – производительность грид-системы имеет сильную зависимость от загруженности каналов связи, что является следствием максимальной территориальной распределённости вычислительного модуля грид-системы среди всех типов информационных систем. Реализация данной угрозы возможна при условии недостаточного контроля за состоянием отдельных узлов грид-системы со стороны диспетчера задач грид-системы	С					Не актуальная	Данная технология не применяется в ИС
48	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через неё на другие системы путём осуществления несанкционированного доступа к образам виртуальных машин. Данная угроза обусловлена слабостями мер разграничения доступа к образам виртуальных машин, реализованных в программном обеспечении виртуализации. Реализация данной угрозы может привести: к нарушению конфиденциальности защищаемой информации, обрабатываемой с помощью виртуальных машин, созданных на основе несанкционированно изменённых образов; к нарушению целостности программ, установленных на виртуальных машинах; к нарушению доступности ресурсов виртуальных машин.	С	ПДН	К	Ущерб субъекту ПДН Репутационный\ Социальный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
49	Угроза нарушения целостности данных кеша	Угроза заключается в возможности размещения нарушителем в кеше приложения (например, браузера) или службы (например, DNS или ARP) некорректных (потенциально опасных) данных таким образом, что до обновления кеша дискредитируемое приложение (или служба) будет считать эти данные корректными. Данная угроза обусловлена слабостями в механизме контроля целостности данных в кеше. Реализация данной угрозы возможна в условиях осуществления нарушителем успешного несанкционированного доступа к данным кеша и отсутствии проверки целостности данных в кеше со стороны дискредитируемого приложения (или службы)	Н	ПДН	Ц	Репутационный	Н	Не актуальная	
					Д	Репутационный	Н		
				СТ	Ц	Технологический Экономический	Н		
					Д	Технологический	Н		
50	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Угроза заключается в возможности искажения информации, сохраняемой в хранилище больших данных, или отказа в проведении сохранения при передаче в него данных в некоторых форматах. Данная угроза обусловлена слабостями технологий определения формата входных данных на основе дополнительной служебной информации (заголовки файлов и сетевых пакетов, расширения файлов и т.п.), а также технологий адаптивного выбора и применения методов обработки мультимедийной 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 содержанию, или в хранилище больших данных не реализованы методы обработки данных получаемого формата	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
51	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Угроза заключается в возможности потери несохранённых данных, обрабатываемых в предыдущей сессии работы на компьютере, а также в возможности потери времени для возобновления работы на компьютере. Данная угроза обусловлена ошибками в реализации программно-аппаратных компонентов компьютера, связанных с обеспечением питания. Реализация данной угрозы возможна при условии невозможности выведения компьютера из промежуточных состояний питания («ждущего режима работы», «гибернации» и др.)	Н	ПДН	Ц	Репутационный	Н	Акту альна я	
					Д	Репутационный	Н		
					Ц	Репутационный Экономический Технологический	С		
					Д	Репутационный Экономический Технологический	Н		
52	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Угроза заключается в возможности возникновения у потребителя облачных услуг непреодолимых сложностей для смены поставщика облачных услуг из-за технических сложностей в реализации процедуры миграции образов виртуальных машин из облачной системы одного поставщика облачных услуг в систему другого. Данная угроза обусловлена тем, что каждый поставщик облачных услуг использует для реализации своей деятельности аппаратное и программное обеспечение различных производителей, часть которого может использовать специфические (для данного производителя) инструкции, протоколы, методы, схемы коммутации и другие особенности реализации своего функционала. Реализация данной угрозы возможна в случае несовместимости стандартных программных интерфейсов обмена данными (API) для реализации процедуры миграции образов виртуальных машин между различными поставщиками облачных услуг в одном или обоих направлениях.	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
53	Угроза невозможности управления правами пользователей BIOS	Угроза заключается в возможности неправомерного использования пользователями декларированного функционала BIOS/UEFI, ориентированного на администраторов. Данная угроза обусловлена слабостями технологий разграничения доступа (распределения прав) к функционалу BIOS/UEFI между различными пользователями и администраторами. Реализация данной угрозы возможна при условии физического доступа к терминалу и, при необходимости, к системному блоку компьютера	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		
54	Угроза недобросовестного исполнения обязательств поставщика облачных услуг	Угроза заключается в возможности раскрытия или повреждения целостности поставщиком облачных услуг защищаемой информации потребителей облачных услуг, невыполнения требований к уровню качества (уровню доступности) предоставляемых потребителям облачных услуг доступа к их программам или иммигрированным в облако информационным системам. Данная угроза обусловлена невозможностью непосредственного контроля над действиями сотрудников поставщика облачных услуг со стороны их потребителей. Реализация данной угрозы возможна в случаях халатности со стороны сотрудников поставщика облачных услуг, недостаточности должностных и иных инструкций данных сотрудников, недостаточности мер по менеджменту и обеспечению безопасности облачных услуг и т.д.	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
55	Угроза незащищённого администрирования облачных услуг	<p>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.</p> <p>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.</p> <p>Реализация данной угрозы возможна в случае получения нарушителем аутентификационной информации (при их вводе в общественных местах) легальных пользователей, или эксплуатации уязвимостей в средствах удалённого администрирования</p>	Н						Данная технология не применяется в ИС
56	Угроза некачественного переноса инфраструктуры в облако	<p>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.</p> <p>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).</p> <p>Реализация данной угрозы возможна в случае несовместимости программных и сетевых интерфейсов или несоответствий политик безопасности при осуществлении переноса информационной системы в облако</p>	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
57	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Угроза заключается в сложности контроля за всеми автоматически создаваемыми копиями информации в хранилище больших данных из-за временной несогласованности данных операций. Данная угроза обусловлена осуществлением дублирования (дву- или многократного) данных на различных вычислительных узлах, входящих в состав хранилища больших данных, с целью повышения скорости доступа к этим данным при большом количестве запросов чтения/записи. При этом данная операция является внутренней функцией и «непрозрачна» для конечных пользователей и администраторов хранилища больших данных. Реализация данной угрозы возможна при условии недостаточности мер по контролю за автоматически создаваемыми копиями информации, применяемых в хранилище больших данных	Н						Данная технология не применяется в ИС
58	Угроза неконтролируемого роста числа виртуальных машин	Угроза заключается в возможности ограничения или нарушения доступности виртуальных ресурсов для конечных потребителей облачных услуг путём случайного или несанкционированного преднамеренного создания нарушителем множества виртуальных машин. Данная угроза обусловлена ограниченностью объёма дискового пространства, выделенного под виртуальную инфраструктуру, и слабостями технологий контроля процесса создания виртуальных машин. Реализация данной угрозы возможна при условии наличия у нарушителя прав на создание виртуальных машин в облачной инфраструктуре	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
59	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Угроза заключается в возможности отказа легальным пользователям в выделении компьютерных ресурсов после осуществления нарушителем неправомерного резервирования всех свободных компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти). 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	Н	ПДН	Д	Репутационный Технологический	С	Актуальна	
				СТ	Д	Технологический	С		
60	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Угроза заключается в возможности удаления из хранилища некоторых обрабатываемых данных без уведомления конечного пользователя или администратора. Данная угроза обусловлена слабостями механизма автоматического удаления данных, не отвечающих определённым требованиям (предельный «срок жизни» в хранилище, конечная несогласованность с другими данными, создание копии в другом месте и т.п.). Реализация данной угрозы возможна при условии недостаточности реализованных в хранилище больших данных мер по контролю за автоматическим удалением данных	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
61	Угроза некорректного задания структуры данных транзакции	Угроза заключается в возможности совершения нарушителем (клиентом базы данных) подлога путём прерывания транзакции или подмены идентификатора транзакции. В первом случае происходит неполное выполнение транзакции, а во втором – пользователь форсированно завершает транзакцию, изменяя её ID, и сообщая о том, что транзакция не была проведена, тем самым провоцируя повторное проведение транзакции. Данная угроза обусловлена слабостями механизма контроля непрерывности транзакций и целостности данных, передаваемых в ходе транзакции между базой данных и её клиентом	С	ПДН	Ц	Репутационный Технологический	С	Актуальная	
					Д	Технологический	С		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический	С		
62	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Угроза заключается в возможности перенаправления или копирования обрабатываемых браузером данных через прозрачный прокси-сервер, подключённый к 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Неактуальная	
				СТ	К	Репутационный	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
63	Угроза некорректно го использован ия функционал а программно го и аппаратного обеспечения	Угроза заключается в возможности использования декларированных возможностей программных и аппаратных средств определённым (нестандартным, некорректным) способом с целью деструктивного воздействия на информационную систему и обрабатываемую ею информацию. Данная угроза связана со слабостями механизма обработки данных и команд, вводимых пользователями. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к программным и аппаратным средствам	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		
64	Угроза некорректно й реализации политики лицензирова ния в облаке	Угроза заключается в возможности отказа потребителям облачных услуг в удалённом доступе к арендуемому программному обеспечению (т.е. происходит потеря доступности облачной услуги SaaS) по вине поставщика облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками лицензирования использования программного обеспечения различных производителей в облаке. Реализация данной угрозы возможна при условии, что политика лицензирования использования программного обеспечения основана на ограничении количества его установок или числа его пользователей, а созданные виртуальные машины с лицензируемым программным обеспечением использованы много раз	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
65	Угроза неопределённости в распределении ответственности между ролями в облаке	Угроза заключается в возможности возникновения существенных разногласий между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей в части обеспечения информационной безопасности. 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)	Н						Данная технология не применяется в ИС
66	Угроза неопределённости ответственности за обеспечение безопасности и облака	Угроза заключается в возможности невыполнения ряда мер по защите информации как поставщиком облачных услуг, так и их потребителем. Данная угроза обусловлена отсутствием чёткого разделения ответственности в части обеспечения безопасности информации между потребителем и поставщиком облачных услуг. Реализация данной угрозы возможна при условии недостаточности документального разделения сфер ответственности между сторонами участвующими в оказании облачных услуг, а также отсутствия документального определения ответственности за несоблюдение требований безопасности	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
67	Угроза неправомерного ознакомления с защищаемой информацией	Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный	Н		
68	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API). 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	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
69	Угроза неправомерных действий в каналах связи	Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных. Реализация данной угрозы возможна при условии осуществления нарушителем несанкционированного доступа к сетевому трафику	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический	Н		
70	Угроза непрерывной модернизации облачной инфраструктуры	Угроза заключается в возможности занесения в облачную систему уязвимостей и слабостей вместе с добавлением нового программного или аппаратного обеспечения. При этом система, рассматриваемая как защищённая на этапе ввода её в эксплуатацию, уже не может считаться таковой после её модернизации. Данная угроза обусловлена тем, что, во-первых, поставщики облачных услуг предоставляют возможность осуществления потребителем облачных услуг выбора и (или) изменения первоначального состава программного обеспечения облачной инфраструктуры в процессе оказания таких услуг, а, во-вторых, при интенсивном подключении новых потребителей модернизация облачной инфраструктуры может проходить несколько раз в год. Реализация данной угрозы возможна в случае, если срок до следующей модернизации не превышает срока проведения оценки соответствия системы требованиям безопасности в условиях отсутствия системы менеджмента облачных услуг и обеспечения их безопасности (системы облачного менеджмента)	С						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
71	Угроза несанкционированного восстановления удалённой защищаемой информации	<p>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.</p> <p>Данная угроза обусловлена слабостями механизма удаления информации с машинных носителей – информация, удалённая с машинного носителя, в большинстве случаев может быть восстановлена.</p> <p>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).</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный	С		
72	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	<p>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.</p> <p>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.</p> <p>Реализация данной угрозы возможна в одном из следующих условий: выключенном механизме защиты BIOS/UEFI от записи; успешной эксплуатации нарушителем уязвимости механизма обновления BIOS/UEFI, приводящей к переполнению буфера</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путём эксплуатации уязвимостей программного и (или) микропрограммного обеспечения указанного оборудования. Данная угроза обусловлена ограниченностью функциональных возможностей (наличием слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры, наличием у данного оборудования фиксированного сетевого адреса. Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный	В		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		
74	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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
75	Угроза несанкционированного доступа к виртуальным каналам передачи	Угроза заключается в возможности осуществления нарушителем несанкционированного перехвата трафика сетевых узлов, недоступных с помощью сетевых технологий, отличных от сетевых технологий виртуализации, путём некорректного использования таких технологий. Данная угроза обусловлена слабостями мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных). Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Актуальная	
				СТ	К	Репутационный	С		
76	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор. 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. 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	С	ПДН	Д	Репутационный Технологический	С	Актуальная	
				СТ	Д	Технологический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
77	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Угроза заключается в возможности нарушения вредоносной программой, функционирующей внутри виртуальной машины, целостности программного кода своей и (или) других виртуальных машин, функционирующих под управлением того же гипервизора, а также изменения параметров её (их) настройки. Данная угроза обусловлена наличием слабостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения не только защищаемой информации и программного кода обрабатывающих её программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной виртуальной машины	С	ПДН	Ц	Репутационный Технологический	Н	Акту альна я	
					Д	Технологический	Н		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
78	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации. Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		
79	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин с помощью различных механизмов обмена данными между виртуальными машинами, реализуемых гипервизором и активированных в системе. Данная угроза обусловлена слабостями механизма обмена данными между виртуальными машинами и уязвимостями его реализации в конкретном гипервизоре. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий, достаточных для использования различных механизмов обмена данными между виртуальными машинами, реализованных в гипервизоре и активированных в системе	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
80	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Угроза заключается в возможности удалённого осуществления нарушителем несанкционированного доступа к виртуальным устройствам из виртуальной и (или) физической сети с помощью различных сетевых технологий, используемых для осуществления обмена данными в системе, построенной с использованием технологий виртуализации. Данная угроза обусловлена наличием слабостей в сетевых программных интерфейсах гипервизоров, предназначенных для удалённого управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий достаточных для осуществления обмена данными в системе, построенной с использованием технологий виртуализации	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альная я	
					Ц	Репутационный Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		
81	Угроза несанкционированного доступа к сегментам вычислительного поля	Угроза заключается в возможности осуществления несанкционированного доступа нарушителя к исходным данным, промежуточным и окончательным результатам расчётов других пользователей суперкомпьютера, а также случайное или преднамеренное деструктивное воздействие процессов решения одних задач на процессы и результаты решения других вычислительных задач. Данная угроза обусловлена слабостями механизма разграничения доступа субъектов к сегментам вычислительных полей суперкомпьютера. Реализация данной угрозы возможна при выполнении задач различных пользователей суперкомпьютера на одном вычислительном поле суперкомпьютера	С	ПДН					Данная технология не применяется в ИС
				СТ					

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
82	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	<p>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.</p> <p>Данная угроза обусловлена наличием уязвимостей в клиенте грид-системы (клиентского программного обеспечения, устанавливаемого в узлах грид-системы), эксплуатация которых позволяет нарушителю осуществлять операции чтения и записи в объектах локальной файловой системы компьютера, отправку сигналов программным процессам (включая сигналы прекращения работы), операции чтения и записи в память программных процессов, соответствующих связующему программному обеспечению и грид-заданиям, открытия сетевых соединений в локальных и внешних узлах грид-системы.</p> <p>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)</p>	С						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
83	Угроза несанкционированного доступа к системе по беспроводным каналам	Угроза заключается в возможности получения нарушителем доступа к ресурсам всей дискредитируемой информационной системы через используемые в её составе беспроводные каналы передачи данных. Данная угроза обусловлена слабостями протоколов идентификации/аутентификации (таких как WEP, WPA и WPA2, 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 приёма сигналов дискредитируемой беспроводной сети	Н						Данная технология не применяется в ИС
84	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.	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
				СТ	К	Репутационный	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
85	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	<p>Угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски (являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путём логического объединения нескольких виртуальных устройств хранения данных).</p> <p>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.</p> <p>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.)</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Технологический Социальный	С		
					Д	Технологический Социальный	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информа ции	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
86	Угроза несанкцион ированного изменения аутентифика ционной информации	Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств. Данная угроза обусловлена наличием слабостей мер разграничения доступа к информации аутентификации. Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учётной записью дискредитированного пользователя	Н	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
					Д	Репутационный Технологический	С		
				СТ	Ц	Репутационный Технологический Экономический	С		
					Д	Репутационный Технологический	С		
88	Угроза несанкцион ированного копирования защищаемой информации	Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне. Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
87	Угроза несанкционированного использования привилегированных функций BIOS	Угроза заключается в возможности использования нарушителем потенциально опасных возможностей BIOS/UEFI. Данная угроза обусловлена наличием в BIOS/UEFI потенциально опасного функционала	Внутренний нарушитель с низким потенциалом	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
			Внешний нарушитель с высоким потенциалом	ПДН	К	Ущерб субъекту ПДН Репутационный	В		
					Ц	Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
89	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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Акту альная я	
					Ц	Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
90	Угроза несанкционированного создания учётной записи пользователя	Угроза заключается в возможности создания нарушителем в системе дополнительной учётной записи пользователя и её дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учётной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации. Реализация данной угрозы возможна в случае наличия и прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Акту альная я	
					Ц	Технологический	С		
					Д	Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
91	Угроза несанкционированного удаления защищаемой информации	Угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации путём осуществления деструктивного программного или физического воздействия на машинный носитель информации. Данная угроза обусловлена недостаточностью мер по обеспечению доступности защищаемой информации в системе, а равно и наличием уязвимостей в программном обеспечении, реализующим данные меры. Реализация данной угрозы возможна в случае получения нарушителем системных прав на стирание данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия	Н	ПДН	Д	Репутационный Технологический	С	Актуальная	
				СТ	Д	Технологический Экономический	С		
92	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Угроза заключается в возможности получения нарушителем привилегий управления системой путём использования удалённого внеполосного (по независимому вспомогательному каналу ТСР/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)	В	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Технологический Репутационный	С		
					Д	Технологический Репутационный	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
93	Угроза несанкционированного управления буфером	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся там информацией или осуществления деструктивного программного воздействия на систему (например, переполнение буфера для выполнения произвольного вредоносного кода). Данная угроза обусловлена слабостями в механизме разграничения доступа к буферу обмена, а также слабостями в механизмах проверки вводимых данных. Реализация данной угрозы возможна в случае осуществления нарушителем успешного несанкционированного доступа к сегменту оперативной памяти дискредитируемого объекта, в котором расположен буфер обмена	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Неактуальная	
					Ц	Технологический	Н		
					Д	Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	Н		
					Д	Технологический Экономический	Н		
95	Угроза несанкционированного управления указателями	Угроза заключается в возможности выполнения нарушителем произвольного вредоносного кода от имени дискредитируемого приложения или приведения дискредитируемого приложения в состояние «отказ в обслуживании» путём изменения указателей на ячейки памяти, содержащие определённые данные, используемые дискредитируемым приложением. Данная угроза связана с уязвимостями в средствах разграничения доступа к памяти и контроля целостности содержимого ячеек памяти. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение указателей, используемых дискредитируемым приложением	С	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Актуальная	
					Ц	Технологический Репутационный	Н		
					Д	Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	Н		
					Д	Технологический Экономический	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
94	Угроза несанкционированного управления синхронизацией и состоянием	<p>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.).</p> <p>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.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя возможности:</p> <ul style="list-style-type: none"> 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) 	С	ПДН	Ц	Репутационный Технологический	В	Акту альна я	
					Д	Репутационный Технологический	В		
				СТ	Ц	Репутационный Технологический Экономический	В		
					Д	Репутационный Технологический	В		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
96	Угроза несогласованности политик безопасности и элементов облачной инфраструктуры	Угроза заключается в возможности осуществления нарушителем деструктивных программных воздействий как в отношении поставщиков, так и потребителей облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками безопасности элементов облачной инфраструктуры вследствие значительной распределённости облачной инфраструктуры. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)	Н						Данная технология не применяется в ИС
97	Угроза несогласованности правил доступа к большим данным	Угроза заключается в возможности предоставления ошибочного неправомерного доступа к защищаемой информации или, наоборот, возможности отказа в доступе к защищаемой информации легальным пользователям в силу ошибок, допущенных при делегировании им привилегий другими легальными пользователями хранилища больших данных. Данная угроза обусловлена недостаточностью мер по разграничению и согласованию доступа к информации различных пользователей в хранилище больших данных. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Угроза заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов. Данная угроза связана с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции сканирования портов и анализа сетевого трафика	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
				СТ	К	Репутационный Социальный	С		
99	Угроза обнаружения хостов	Угроза заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции анализа сетевого трафика	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Акту альная я	
					Ц	Технологический Репутационный	С		
					Д	Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		
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	С						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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	С	ПДН	Ц	Технологический Репутационный	В	Акту альна я	
					Д	Технологический Репутационный	С		
				СТ	Ц	Технологический Экономический	В		
					Д	Технологический Экономический	С		
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 межсетевое 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.)	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Неакт уальн ая	
				СТ	К	Социальный Репутационный	Н		

Продолжение таблицы Г.8

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
104	Угроза определения топологии вычислительной сети	<p>Угроза заключается в возможности определения нарушителем состояния сетевых узлов дискредитируемой системы (т.н. сканирование сети) для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз.</p> <p>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).</p> <p>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</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Неактуальная	
				СТ	К	Социальный Репутационный	Н		
105	Угроза отказа в загрузке входных данных неизвестного формата хранения больших данных	<p>Угроза заключается в возможности отказа хранилищем больших данных в приеме входных данных неизвестного формата от легального пользователя.</p> <p>Данная угроза обусловлена отсутствием в хранилище больших данных механизма самостоятельной (автоматической) адаптации к новым форматам данных.</p> <p>Реализация данной угрозы возможна при условии поступления запроса на загрузку в хранилище входных данных неизвестного формата</p>	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
106	Угроза отказа в обслуживании системы 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	Н						Данная технология не применяется в 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.). 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							Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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 от работоспособности гипервизора. Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора: сбоях в процессе его обновления, обновлений, в ходе которых внедряются новые ошибки в код гипервизора, обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования либо других инцидентов безопасности информации	Н	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
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 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 отличие от других подобных угроз, нарушитель действует «вслепую» – простым путём перебора всевозможных комбинаций	С	ПДН	Ц	Репутационный Технологический	С	Актуальная	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
110	Угроза перегрузки грид-системы вычислительными заданиями	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 от работоспособности гипервизора. Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора: сбоев в процессе его обновления, обновлений, в ходе которых внедряются новые ошибки в код гипервизора, обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования либо других инцидентов безопасности информации	Н						Данная технология не применяется в ИС
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. 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	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
111	Угроза передачи данных по скрытым каналам	<p>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.</p> <p>Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных.</p> <p>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; доступа к каналам передачи данных; посещении пользователем сайтов в сети Интернет и открытия электронных писем, содержащих скрытые пиксели</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Слциальный	Н		
113	Угроза перезагрузк и аппаратных и программно-аппаратных средств вычислительной техники	<p>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.</p> <p>Данная угроза обусловлена свойством оперативной памяти обнулять своё состояние при выключении и перезагрузке.</p> <p>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 на осуществление форсированной перезагрузки</p>	Н	ПДН	Ц	Технологический Репутационный	В	Актуальная	
					Д	Технологический Репутационный	С		
				СТ	Ц	Технологический Экономический	В		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информа ции	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
114	Угроза переполнени я целочисленн ых переменных	Угроза заключается в возможности приведения нарушителем дискредитируемого приложения к сбоям в работе путём подачи на его входные интерфейсы данных неподдерживаемого формата или выполнения с его помощью операции, в результате которой будут получены данные неподдерживаемого дискредитируемым приложением формата. Данная угроза обусловлена уязвимостями программного обеспечения, связанными с недостаточной проверкой такими приложениями корректности входных данных, а также тем, что операторы любого программного обеспечения способны правильно обрабатывать только определённые типы данных (например, только целые или только положительные числа). Реализация данной угрозы возможна при условии наличия у нарушителя: сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных; возможности взаимодействия с входным интерфейсом дискредитируемого приложения	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	<p>Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информации, вводимой и выводимой на периферийные устройства, путём перехвата данных, обрабатываемых контроллерами периферийных устройств.</p> <p>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).</p> <p>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.</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информа ции	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
116	Угроза перехвата данных, передаваемых по вычислитель ной сети	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном (иногда в активном) режиме (т.е. «прослушивать сетевой трафик») для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы невидимым (скрытным) получателем перехватываемых данных. Кроме того, нарушитель может проводить исследования других типов потоков данных, например, радиосигналов. Данная угроза обусловлена слабостями механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибками конфигурации сетевого программного обеспечения. Реализация данной угрозы возможна в следующих условиях: наличие у нарушителя доступа к дискредитируемой вычислительную сети; неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информа ции	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
118	Угроза перехвата привилегированного процесса	<p>Угроза заключается в возможности получения нарушителем права управления процессом, обладающим высокими привилегиями (например, унаследованными от пользователя или группы пользователей, выполняющих роль администраторов дискредитируемой системы), для выполнения произвольного вредоносного кода с правами дискредитированного процесса.</p> <p>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.</p> <p>Реализация данной угрозы возможна при выполнении одного из условий:</p> <ul style="list-style-type: none"> 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 	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
119	Угроза перехвата управления гипервизором	<p>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.</p> <p>Данная угроза обусловлена наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью управления гипервизором</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
120	Угроза перехвата управления средой виртуализации	<p>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.</p> <p>Данная угроза обусловлена наличием у консоли средства управления виртуальной инфраструктурой, реализуемого в рамках одной из виртуальных машин, программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня управления виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью средства управления виртуальной инфраструктурой</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный Социальный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
121	Угроза повреждения системного реестра	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> возникновения ошибок в работе отдельных процессов или всей операционной системы; наличии у нарушителя прав доступа к реестру или файлам, содержащим в себе данные реестра 	Н	ПДН	Ц	Репутационный Технологический	В	Актуальна	
					Д	Репутационный Технологический	В		
				СТ	Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
123	Угроза подбора пароля BIOS	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI путём входа в консоль BIOS/UEFI по паролю, подобранному программно или «вручную» с помощью методов тотального перебора вариантов или подбора по словарю. Данная угроза обусловлена слабостями механизма аутентификации, реализуемого в консолях BIOS/UEFI. Реализация данной угрозы возможна в одном из следующих случаев: 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Актуальная	
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
124	Угроза подделки записей журнала регистрации событий	Угроза заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о не произошедших событиях) для введения в заблуждение её администраторов или сокрытия следов реализации других угроз. Данная угроза обусловлена недостаточностью мер по разграничению доступа к журналу регистрации событий безопасности. Реализация данной угрозы возможна в одном из следующих случаев: технология ведения журналов регистрации событий безопасности предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями; технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования, но нарушитель обладает привилегиями, необходимыми для осуществления записи в файлы журналов, а также специальными программными средствами, способными обрабатывать файлы журналов используемого в дискредитируемой системе формата	Н	ПДН	Ц	Репутационный Технологический	Н	Акту альна я	
				СТ	Ц	Технологический Экономический	С		
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	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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, 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	Н						Данная технология не применяется в ИС
275	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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	Н		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	Н		
					Д	Технологический Экономический	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
128	Угроза подмены доверенного пользователя	<p>Угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента».</p> <p>Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника/получателя информации.</p> <p>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.</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Не актуальная	
				СТ	К	Репутационный Социальный	Н		
129	Угроза подмены резервной копии программного обеспечения BIOS	<p>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.</p> <p>Данная угроза обусловлена недостаточностью мер разграничения доступа и контроля целостности резервных копий программного обеспечения BIOS/UEFI.</p> <p>Реализация данной угрозы возможна в следующих условиях: нарушитель успешно подменил резервную копию программного обеспечения BIOS/UEFI; возникла необходимость восстановления предыдущей версии программного обеспечения BIOS/UEFI (данное условие может произойти как случайно, так и быть спровоцировано нарушителем)</p>	Н	ПДН	Ц	Репутационный Технологический	Н	Не актуальная	
				СТ	Ц	Технологический Экономический	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Социальный	С		
131	Угроза подмены субъекта сетевого доступа	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены в отправляемых дискредитируемым пользователем сетевых запросах сведений об отправителе сообщения. Данную угрозу можно охарактеризовать как «имитация действий сервера». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника информации. Реализация данной угрозы возможна при условии успешной выдачи себя нарушителем за законного отправителя (например, с помощью ложных фишинговых веб-сайтов). Ключевое отличие от «угрозы подмены содержимого сетевых ресурсов» заключается в том, что в данном случае нарушитель не изменяет оригинального содержимого электронного ресурса (веб-сайта, электронного письма), а только служебные сведения	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Технологический Репутационный	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Репутационный	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
132	Угроза получения предварительной информации об объекте защиты	<p>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.</p> <p>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.).</p> <p>Реализация данной угрозы возможна при условии получения информации о дискредитируемой системе с помощью хотя бы одного из следующих способов изучения дискредитируемой системы:</p> <p>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)</p> <p>анализ реакций системы на строковые URI-запросы (в т.ч. неверные SQL-запросы, альтернативные пути доступа к файлам).</p> <p>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</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
133	Угроза получения сведений о владельце беспроводного устройства	<p>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.</p> <p>Данная угроза обусловлена слабостью защиты идентификационной информации беспроводных точек доступа при их подключении к сети Интернет.</p> <p>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</p>							Данная технология не применяется в ИС
135	Угроза потери и утечки данных, обрабатываемых в облаке	<p>Угроза заключается в возможности нарушения конфиденциальности, целостности и доступности защищаемой информации потребителей облачных услуг, обрабатываемой в облачной системе.</p> <p>Данная угроза обусловлена слабостями мер защиты информации, обрабатываемой в облачной системе.</p> <p>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</p>							Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
134	Угроза потери доверия к поставщику облачных услуг	<p>Угроза заключается в возможности снижения уровня защищённости и допущения дополнительных ошибок в обеспечении безопасности защищаемой в облачной системе информации из-за невозможности оттока у поставщика облачных услуг необходимых ресурсов в связи с потерей потребителями облачных услуг доверия к их поставщику.</p> <p>Данная угроза обусловлена тем, что из-за обнародования фактов об инцидентах информационной безопасности, связанных с поставщиком облачных услуг, происходит потеря доверия к такому поставщику со стороны потребителей облачных услуг, и, как следствие, возникает необходимость лавинообразного выделения поставщиком облачных услуг ресурсов (человеческих, технических, финансовых) для решения возникающих в данной ситуации задач (множественные консультации пользователей, экстренный пересмотр политик безопасности, модернизация системы защиты и др.), что не только может вызвать нехватку ресурсов для обеспечения текущего уровня защищённости информации, но и спровоцировать допуск «в спешке» новых ошибок.</p> <p>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</p>	С						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Угроза заключается в возможности допуска ошибок при копировании защищаемой информации при распределённом хранении данных на различных узлах хранилища больших данных вследствие несогласованности их работы, влекущих за собой невозможность осуществления легальным пользователем доступа к блокам или ко всей защищаемой информации. Данная угроза обусловлена слабостями механизмов репликации данных, реализованных в узлах хранилища больших данных. Реализация данной угрозы возможна в условиях отключения или вывода 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	Н						Данная технология не применяется в 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. Данная угроза обусловлена сложностью определения логического и физического местоположения облачных ресурсов, недостаточностью мер физического контроля доступа к хранилищам данных, резервного копирования и др., а также необходимостью учёта особенностей законодательства в области защиты информации стран, резидентами которых являются поставщики облачных услуг, выполняющих роль субподрядчиков по оказанию заказанных облачных услуг. Реализация данной угрозы возможна при условии, что выполнение требований к функционалу облачной системы затрудняется из-за правовых норм других стран, участвующих в трансграничной передаче облачного трафика							Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
138	Угроза потери управления собственной инфраструктурой при переносе её в облако	<p>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.</p> <p>Данная угроза обусловлена невозможностью достоверной оценки потребителем облачных услуг реального уровня защищённости, обеспечиваемого поставщиком облачных услуг в отношении защищаемой информации потребителя облачных услуг, в связи с закрытостью для потребителей сведений о применяемых поставщиком облачных услуг технологиях, программных и технических решениях, а также конкретных параметрах настроек средств защиты информации.</p> <p>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)</p>	С						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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.)	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	В		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		
140	Угроза приведения системы в состояние «отказ в обслуживании»	Угроза заключается в возможности отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой 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 сетевых протоколов	Н	ПДН	Д	Репутационный Технологический	В	Акту альна я	
				СТ	Д	Технологический Экономический	В		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
141	Угроза привязки к поставщику облачных услуг	Угроза заключается в возможности возникновения трудно решаемых (или даже неразрешимых) проблем технического, организационного, юридического или другого характера, препятствующих осуществлению потребителем облачных услуг смены их поставщика. Данная угроза обусловлена отсутствием совместимости между форматами данных и программными интерфейсами, используемыми в облачных инфраструктурах различных поставщиков облачных услуг. Реализация данной угрозы возможна при условии использования поставщиком облачных услуг нестандартного программного обеспечения или формата образов виртуальных машин и отсутствием средств преобразования образа виртуальной машины из используемого им формата в другой (используемый другим поставщиком)	Н						Данная технология не применяется в ИС
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							Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
143	Угроза программного вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	<p>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.</p> <p>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).</p> <p>Реализация данной угрозы возможна при наличии у нарушителя прав на отправку команды или специально сформированных входных данных на средства хранения, обработки и (или) ввода/вывода/передачи информации</p>	С	ПДН	Ц	Репутационный Технологический	В	Актуальна	
					Д	Репутационный Технологический	В		
				СТ	Ц	Технологический Экономический	В		
					Д	Технологический Экономический	В		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
144	Угроза программно го 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Акту альная я	
					Ц	Технологический Репутационный	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технолгический Репутационный	С		
145	Угроза прямого обращения к памяти вычислитель ного поля суперкомпь ютера	Угроза заключается в возможности осуществления процессом нарушителя, функционирующем в вычислительном поле суперкомпьютера, считывания защищаемых данных из оперативной памяти, выделенной для параллельного (дискредитируемого) процесса, с использованием операций удалённого прямого доступа к памяти. Данная угроза обусловлена слабостями протокола прямого доступа к оперативной памяти, с помощью которого выполняется обращение к сегменту памяти, выделенному для удалённого параллельного процесса, функционирующего в вычислительном поле суперкомпьютера. Реализация данной угрозы возможна при условии успешного осуществления нарушителем доступа к входным/выходным данным параллельных процессов в вычислительном поле суперкомпьютера	С						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
146	Угроза пропуска проверки целостности программного обеспечения	<p>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.</p> <p>Данная угроза обусловлена слабостями механизмов проверки целостности файлов программного обеспечения и/или проверки подлинности источника их получения.</p> <p>Реализация данной угрозы возможна при условии успешного использования обманных техник одного из следующих методов:</p> <p>«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);</p> <p>«автоматического метода» – нарушитель осуществляет деструктивное воздействие переадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер</p>	Н	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С						Данная технология не применяется в 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» 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							Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
149	Угроза сбоя обработки специальными 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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
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)	С	ПДН	Д	Репутационный Технологический	С	Акту альна я	
				СТ	Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Не актуальная	
				СТ	К	Репутационный Социальный	Н		
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	Н		

Продолжение таблицы Г.8

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на дискредитируемую систему большим объемом сетевого трафика, генерируемого сторонними серверами в ответ на сетевые запросы нарушителя, сформированные от имени дискредитируемой системы. Генерируемый сторонними серверами сетевой трафик значительно превышает объем 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	Н	ПДН	Д	Репутационный Технологический	С	Актуальная	
				СТ	Д	Технологический Экономический	С		
154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Угроза заключается в возможности внесения уязвимостей в программное обеспечение BIOS/UEFI в ходе его обновления, которые могут быть использованы в дальнейшем для приведения компьютера в состояние «отказ в обслуживании», несанкционированного изменения конфигурации BIOS/UEFI или выполнения вредоносного кода при каждом запуске компьютера. Данная угроза обусловлена слабостями мер контроля отсутствия уязвимостей в только что вышедших версиях обновления программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Технологический	С		
					Д	Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
155	Угроза утраты вычислительных ресурсов	<p>Угроза заключается в возможности отказа легитимному пользователю в выделении ресурсов для обработки его запросов из-за истощения нарушителем свободных ресурсов в системе, осуществлённого путём их несанкционированного исключения из общего пула ресурсов на основе техник «утечки ресурсов» или «выделения ресурсов».</p> <p>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.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя:</p> <p>сведений о формате и параметрах деструктивных воздействий на систему, приводящих к исключению («утечки» или «выделению») свободных ресурсов из общего пула ресурсов дискредитируемой системы;</p> <p>привилегий, достаточных для осуществления деструктивных воздействий («утечки» или «выделения») в дискредитируемой системе;</p> <p>отсутствия 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</p>	Н	ПДН	Д	Репутационный Технологический	С	Актуальная	
				СТ	Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	Н	ПДН	К	Репутационный Ущерб субъекту ПДН	С	Актуальная	
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	С		
					Д	Технологический Экономический	Н		
157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угроза заключается в возможности умышленного выведения из строя внешним нарушителем средств хранения, обработки и (или) ввода/вывода/передачи информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Н	ПДН	Ц	Репутационный Технологический	С	Актуальная	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
158	Угроза форматирования носителей информации	Угроза заключается в возможности утраты хранящейся на формируемом 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.	Н	ПДН	Ц	Репутационный Технологический	С	Акту альна я	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
159	Угроза «форсированного веб-браузинга»	Угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации «ручного ввода» в адресную строку веб-браузера определённых адресов веб-страниц и осуществления принудительного перехода по дереву веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
				СТ	К	Репутационный Социальный	С		

Продолжение таблицы Г.8

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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.)	Н	ПДН	К	Репутационный Ущерб субъекту ПДН	В	Актуальная	
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Д	Технологический Экономический	Н		
161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Угроза заключается в возможности возникновения ситуации типа «отказ в обслуживании» со стороны вычислительного поля суперкомпьютера. Данная угроза обусловлена слабостями мер контроля за распределением вычислительных ресурсов суперкомпьютера при обработке задачи несколькими процессорами. Реализация данной угрозы возможна при условии выполнения суперкомпьютером специфичных вычислительных задач, в ходе которых генерируются межпроцессорные сообщения с большой интенсивностью	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
162	Угроза эксплуатации и цифровой подписи программного кода	Угроза заключается в возможности повышения нарушителем привилегий в системах, использующих цифровую подпись кода в качестве связующей информации между программой и её привилегиями, путём дискредитации механизма подписывания программного кода. Данная угроза обусловлена слабостями в механизме подписывания программного кода. Реализация данной угрозы возможна при следующих условиях: дискредитируемый программный код написан с помощью фреймворка (framework), поддерживающего подписывание программного кода; дискредитируемый программный код подписан вендором (поставщиком программного обеспечения); нарушитель имеет возможность внедрить программный код в дискредитируемый компьютер	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		
163	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 уровне 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»	Н						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
164	Угроза перехвата исключения/сигнала из привилегированного блока функций	<p>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.</p> <p>Данная угроза обусловлена тем, что вызов программных функций в привилегированном режиме подразумевает отключение для них механизмов разграничения доступа.</p> <p>Реализация данной угрозы возможна при следующих условиях:</p> <p>дискредитируемая программа, написана на языке программирования, поддерживающего механизм привилегированных блоков (например, Java);</p> <p>в дискредитируемой программе вызов привилегированных блоков осуществлён небезопасным способом (использовано публичное объявление внутренних функций, использована генерация исключений из привилегированного блока);</p> <p>нарушитель обладает правами, достаточными для перехвата программных исключений в системе</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
165	Угроза включения в проект не достоверно испытанных компонентов	Угроза заключается в возможности нарушения безопасности защищаемой информации вследствие выбора для применения в системе компонентов не в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др. Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии выбора применения в системе компонентов по цене, разрекламированности и др.	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический Экономический	Н		
166	Угроза внедрения системной избыточност и	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)	С	ПДН	Д	Репутационный Технологический	С	Акту альна я	
				СТ	Д	Технологический Экономический	В		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Угроза заключается в возможности нарушения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест (намеренно или при случайном перенаправлении) сайтов с неблагонадёжным содержимым и запускаемыми с привилегиями дискредитированных пользователей. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов с неблагонадёжным содержимым	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Акту альная я	
					Ц	Технологический Репутационный	В		
					Д	Технологический	В		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		
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, 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; наличия у нарушителя сведений об адресе электронной почты, с которым связана учётная запись дискредитируемого пользователя для доступа к сетевым сервисам	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альная я	
					Д	Технологический Репутационный	В		
				СТ	К	Репутационный Социальный	С		
					Д	Технологический	В		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Акту альная я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	Н		
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	Н	ПДН	Д	Репутационный Технологический	С	Акту альная я	
				СТ	Д	Технологический	С		

Продолжение таблицы Г.8

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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, 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. 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	Н	ПДН	Д	Репутационный Технологический	С	Актуальная	
				СТ	Д	Технологический	В		
172	Угроза распространения «почтовых червей»	Угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми при получении пользователями системы электронных писем, содержащих вредоносную программу типа «почтовый червь», а также невольного участия в 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический	С		
					Д	Технологический	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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, онлайн-сервисы отправки SMS-сообщений, онлайн-сервисы голосования и др.	Н	ПДН	Д	Репутационный Технологический	С	Актуальная	
				СТ	Д	Технологический	С		
174	Угроза «фарминга»	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией пользователя путём скрытного перенаправления пользователя на поддельный сайт, 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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
				СТ	К	Репутационный Социальный	Н		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
175	Угроза «фишинга»	<p>Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём убеждения его с помощью методов социальной инженерии (в т.ч. посылкой целевых писем (т.н. spear-phishing attack), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений (fake offers) или различных приложений (fake apps)) зайти на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть заражённое вложение в письме.</p> <p>Данная угроза обусловлена недостаточностью знаний пользователей о методах и средствах «фишинга».</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя:</p> <ul style="list-style-type: none"> 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.). <p>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)</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
				СТ	К	Репутационный Социальный	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушения	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Угроза заключается в возможности приведения системы в состояние «отказ в обслуживании» или нарушения штатного режима функционирования из-за временной задержки в системах реального времени, вносимой в процессы передачи и обработки защищаемой информации средствами защиты информации, вызванной необходимостью обработки передаваемой/обрабатываемой информации на предмет выявления и нейтрализации угроз безопасности информации. На реализацию данной угрозы влияет не только номенклатура применяемых средств защиты информации, параметры их настройки, объём передаваемой/обрабатываемой информации, а также текущая активность внешних нарушителей, программные воздействия которых обрабатываются средствами защиты информации	Н	ПДН	Д	Репутационный Технологический	Н	Актуальна	
				СТ	Д	Технологический	С		
177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Угроза заключается в возможности возникновения ошибок в работе системы вследствие отсутствия (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора, средства учёта нижних/верхних пределов скорости и направления реакции оператора, схемы реагирования на двойное нажатие клавиш при вводе обычных и критических данных, процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.). 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 требованиями и фактическим уровнем обнаружения и исправления ошибок	Н	ПДН	Ц	Репутационный Технологический	Н	Актуальна	
					Д	Репутационный Технологический	Н		
				СТ	Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альная я	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный Социальный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	Н		
179	Угроза несанкционированной модификации и 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	Н	ПДН	Ц	Репутационный Технологический	С	Акту альная я	
				СТ	Ц	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С	ПДН	Д	Репутационный Технологический	В	Актуальна	
				СТ	Д	Технологический	В		
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	С	ПДН	Ц	Репутационный Технологический	С	Актуальна	
				СТ	Ц	Технологический Экономический	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
182	Угроза физического устаревания аппаратных компонентов	Угроза заключается в возможности нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозионных субстанций). Возможность реализации данной угрозы возрастает при использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем	Н	ПДН	Д	Репутационный Технологический	С	Актуальна	
				СТ	Д	Технологический	С		
183	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Угроза заключается в возможности осуществления нарушителем сбора и анализа информации, обрабатываемой с помощью мобильного устройства, за счёт использования специального программного обеспечения, встраиваемого пользователем в системное программное обеспечение мобильного устройства, а также встраиваемого в мобильные программы под видом программной платформы для их разработки другими компаниями. Данная угроза обусловлена наличием в мобильном устройстве множества каналов передачи данных, а также сложностью контроля потоков информации в таком устройстве. Реализация данной угрозы возможна при условии использования мобильных устройств пользователями. В качестве собираемой информации могут выступать: персональные данные пользователя и контактирующих с ним лиц (пол, возраст, религиозные и политические взгляды и др.); информация ограниченного доступа (история браузера, список контактов пользователя, история звонков и др.); видеоданные, снимаемые видеокамерами мобильного устройства; аудиоданные, снимаемые микрофоном устройства	С						Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
184	Угроза перехвата управления автоматизированной системой управления технологическими процессами	<p>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.</p> <p>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.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с автоматизированной системой управления технологическими процессами. Реализация данной угрозы может привести к:</p> <p>блокированию или искажению (некорректность выполнения) алгоритмов отработки заданий управления технологическими процессами, непосредственного управления оборудованием предприятия;</p> <p>нарушению штатного хода технологических процессов;</p> <p>частичному или полному останову технологических процессов без (или с) выхода(-ом) оборудования из строя;</p> <p>аварийной ситуации в критической системе информационной инфраструктуры</p>							Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	С		
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	Н	ПДН	Ц	Репутационный Технологический	С	Актуальная	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	Н		
					Д	Технологический	Н		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	Н		
				СТ	К	Репутационный	Н		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		
188	Угроза подмены программно-го обеспечения	Угроза заключается в возможности осуществления нарушителем внедрения в систему вредоносного программного обеспечения за счёт загрузки и установки вредоносного программного обеспечения, скрытого под видом легитимного свободно распространяемого программного обеспечения. 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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	Н	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С	ПДН	Ц	Репутационный Технологический	С	Актуальная	
					Д	Репутационный Технологический	С		
				СТ	Ц	Технологический Экономический	Н		
					Д	Технологический	С		
190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Угроза заключается в возможности осуществления нарушителем внедрения вредоносного кода в компьютер пользователя при посещении зараженных сайтов. Нарушитель выявляет наиболее посещаемые пользователем сайты, затем их взламывает и внедряет в них вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты, а также отсутствием правил межсетевого экранирования. Реализация данной угрозы возможна при: неограниченном доступе пользователя в сеть Интернет; наличии у нарушителя сведений о сайтах, посещаемых пользователем	С	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Угроза заключается в возможности осуществления нарушителем заражения системы путем установки дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты. Реализация данной угрозы возможна при: применении пользователем сторонних дистрибутивов; отсутствии антивирусной проверки перед установкой дистрибутива	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Актуальная	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		
192	Угроза использования уязвимых версий программного обеспечения	Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения. Данная угроза обусловлена слабостями механизмов анализа программного обеспечения на наличие уязвимостей. Реализация данной угрозы возможна при отсутствии проверки перед применением программного обеспечения на наличие в нем уязвимостей	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	В		
				СТ	К	Репутационный	В		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
				СТ	К	Репутационный Социальный	В		
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	В						Не применима к рассматриваемой системе

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	В	ПДН	Ц	Технологический Репутационный	В	Актуальна	
				СТ	Ц	Технологический Экономический	В		
196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Угроза заключается в возможности использования вредоносной программы для контроля списка приложений, запущенных на мобильном устройстве. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносных программ (отсутствие контроля разрешенного программного обеспечения). Реализация данной угрозы возможна при условии, что вредоносная программа внедрена на мобильном устройстве и непреднамеренно запущена самим пользователем	В						Не применима к рассматриваемой системе

Продолжение таблицы Г.8

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
				СТ	К	Репутационный Социальный	С		
198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Угроза заключается в возможности скрытного создания внедренной вредоносной программой учетных записей с правами администратора с целью последующего их использования для несанкционированного доступа к пользовательской информации и к настройкам программного обеспечения, установленного на инфицированном компьютере. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения). Кроме того, данная угроза обусловлена недостаточностью мер по разграничению доступа (контроль создания учетных записей пользователей). Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт	С	ПДН	Ц	Репутационный Технологический	С	Актуальная	
				СТ	Ц	Технологический Экономический	С		

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Угроза заключается в возможности управления мобильным устройством и запущенными на нем приложениями от имени легального пользователя за счет передачи этих команд через виртуальных голосовых ассистентов (например, через Siri для iPhone). Данная угроза обусловлена проблемами аутентификации пользователя, в частности по Voice ID. Голосовой ассистент не может быть полностью уверен в том, что обращающийся к нему голос принадлежит владельцу устройства, поэтому для удобства пользователей и гарантии срабатывания устанавливается низкая чувствительность Voice ID. Это позволяет нарушителю использовать записанную на диктофон речь владельца мобильного устройства. Реализация данной угрозы возможна при условии, что виртуальный голосовой ассистент находится в активном состоянии (то есть, не отключен) и установлена низкая чувствительность голосового идентификатора							Не применима к рассматриваемой системе
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							Не применима к рассматриваемой системе

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Угроза заключается в возможности утечки пользовательских данных за счет использования реализованной в браузерах функции автоматического заполнения 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	С	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
				СТ	К	Репутационный Социальный	В		
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 вредоносной программы, способной запустить виртуальную машину и установить в эту виртуальную машину приложение							Не применима к рассматриваемой системе

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обработ ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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, 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							Не применима к рассматриваемой системе
204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Угроза заключается в возможности несанкционированного изменения вредоносной программой значений параметров контроля и управления исполнительными устройствами в программируемых логических контроллерах после ее проникновения и авторизации на данных устройствах. Реализация угрозы обусловлена возможностью вредоносной программы обнаруживать в сети программируемые логические контроллеры, проникать и функционировать в операционной системе программируемых логических контроллеров, а также недостатками механизмов аутентификации. Реализация данной угрозы возможна при условии, что существует возможность доступа к элементам автоматизированной системы управления технологическими процессами по сети Интернет							Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потен циал наруш ителя	Вид обрабат ываемой информа ции	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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	Н	ПДН	Д	Репутационный Технологический	С	Акту альна я	
				СТ	Д	Технологический	С		
206	Угроза отказа в работе оборудования из-за изменения геолокационн ой информации о нем	Угроза заключается в прекращении работы оборудования с ЧПУ, вызванном изменением геолокационной информации о данном оборудовании. Угроза обусловлена геолокационной привязкой оборудования с ЧПУ к конкретной географической координате при пуско-наладочных работах. Угроза реализуется при условии перемещения оборудования с ЧПУ и приводит к невозможности его дальнейшей эксплуатации							Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угрозы	Название угрозы	Описание угрозы	Потенциал нарушителя	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
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							Данная технология не применяется в ИС

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потенци ал нарушит еля	Вид обраба тывае мой инфор мации	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
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 программы; мер по ограничению программной среды, что позволяют нарушителю осуществлять бесконтрольный запуск программных компонентов.	Внутренний с низким потенциалом	ПДН	Д	Технологический Репутационный	С	Акту альна я	
				СТ	Д	Технологический Экономический	С		
			Внутренний со средним потенциалом	ПДН	Д	Технологический Репутационный	В		
				СТ	Д	Технологический Экономический	В		
			Внешний с низким	ПДН	Д	Технологический Репутационный	С		
				СТ	Д	Технологический Экономический	С		
			Внешний со средним	ПДН	Д	Технологический Репутационный	В		
				СТ	Д	Технологический Экономический	В		

Продолжение таблицы Г.8

№ угр озы	Название угрозы	Описание угрозы	Потенци ал нарушит еля	Вид обраба тывае мой инфор мации	Нарушаем ые свойства безопасно сти информац ии	Вид ущерба	Степ ень ущер ба	Акту ально сть угроз ы	Обоснован ие
209	Угроза несанкциони рованного доступа к защищаемой памяти ядра процессора	<p>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.</p> <p>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:</p> <p>1) отсутствие проверки прав доступа процесса к читаемым областям при спекулятивном выполнении операций, в том числе при чтении из оперативной памяти;</p> <p>2) отсутствие очистки кэша от результатов ошибочного спекулятивного исполнения;</p> <p>3) хранение данных ядра операционной системы в адресном пространстве процесса.</p> <p>Реализация данной угрозы возможна из-за наличия процессоров, имеющих аппаратные уязвимости и отсутствия соответствующих обновлений</p>	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	С	Акту альна я	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		

Продолжение таблицы Г.8

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушения	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
323	210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	В	ПДН	Ц	Технологический Репутационный	В	Актуальная	
					Д	Технологический Репутационный	В		
				СТ	Ц	Технологический Экономический	В		
					Д	Технологический	В		
	211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Н	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Технологический Репутационный	С		
				СТ	К	Репутационный Социальный	С		
					Ц	Технологический Экономический	В		

Продолжение таблицы Г.8

№ угроз	Название угрозы	Описание угрозы	Потенциал нарушения	Вид обрабатываемой информации	Нарушаемые свойства безопасности информации	Вид ущерба	Степень ущерба	Актуальность угрозы	Обоснование
212	Угроза перехвата управления информационной системой	<p>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.</p> <p>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.</p> <p>Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия со средствами централизованного управления</p>	С	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный Технологический	В		
					Д	Репутационный Технологический	В		
				СТ	К	Репутационный Социальный	В		
					Ц	Технологический Экономический	В		
					Д	Технологический	В		
213	Угроза обхода многофакторной аутентификации	<p>Угроза заключается в возможности обхода многофакторной аутентификации путем внедрения вредоносного кода в дискредитируемую систему и компоненты, участвующие в процедуре многофакторной аутентификации.</p> <p>Данная угроза обусловлена:</p> <p>наличием уязвимостей программного обеспечения;</p> <p>слабостями мер антивирусной защиты и разграничения доступа.</p> <p>Реализация данной угрозы возможна:</p> <p>в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников;</p> <p>при наличии у него привилегий установки программного обеспечения</p>	В	ПДН	К	Ущерб субъекту ПДН Репутационный	В	Актуальная	
					Ц	Репутационный Технологический	С		
					Д	Репутационный Технологический	С		
				СТ	К	Репутационный	С		
					Ц	Технологический Экономический	С		
					Д	Технологический	С		

