

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет» РТУ МИРЭА

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Модель угроз безопасности информации

по дисциплине

«Управление информационной безопасностью»

Группа: ББМО-01-22 Выполнила: Огольцова Н.Д.

Проверил: Пимонов Р.В.

Содержание

1 Общие положения
1.1. Назначение Модели угроз
1.2. Нормативно-правовые акты, методические документы, используемые для оценки угроз безопасности информации и разработки Модели угроз
1.3. Наименование обладателя информации, заказчика, оператора систем и сетей
1.4. Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей
1.5. Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии)
2 Описание системами сетей и их характеристика как объектов защиты 6
2.1. Наименование систем и сетей, для которых разработана модель угроз безопасности информации:
2.2. Нормативно правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети
2.3. Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим; основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сети
2.5. Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сети:
2.6. Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа в состав групп пользователей включается все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация)
3 Виды тактик, применяемых нарушителем
4. Возможные объекты воздействия угроз безопасности информации. Возможные негативные последствия реализации угроз безопасности информации. Источники угроз безопасности информации. Способы реализации угроз безопасности информации

Перечень принятых сокращений

АИС Автоматизированная информационная система

БД База данных

ИС Информационная система

НСД Несанкционированный доступ к информации

ОС Операционная система

ПДн Персональные данные

ПО Программное обеспечение

СЗПДн Система защиты персональных данных

СВ Система видеонаблюдения

УБИ Угроза безопасности информации

1 Общие положения

1.1. Назначение Модели угроз

Разработка Модели угроз выполняется для определения актуальных угроз безопасности защищаемой информации, обрабатываемой в ООО «Вкусно и Ладно».

Результаты определения актуальных угроз безопасности защищаемой информации предназначены для формирования обоснованных требований к составу и содержанию мер по обеспечению информационной безопасности ООО «Вкусно и Ладно».

1.2. Нормативно-правовые акты, методические документы, используемые для оценки угроз безопасности информации и разработки Модели угроз

Определение угроз безопасности информации осуществлялось на основании Технических требований, действующего законодательства Российской Федерации. В перечень используемых нормативных источников входят, но не ограничиваются ими:

- Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01 ноября
 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методика оценки угроз безопасности информации ФСТЭК России,
 утвержденная ФСТЭК России 5 февраля 2021 г

- «Требования к системам обнаружения вторжений» (утвержден приказом ФСТЭК России от 06.12.2011 N 638. ДСП);
- «Требования к средствам антивирусной защиты» (утвержден приказом ФСТЭК России от 20.03.2012 N 28. ДСП);
- «Требования к средствам доверенной загрузки» (утвержден приказом ФСТЭК России от 27.09.2013 N 119. ДСП);
- «Требования к межсетевым экранам» (утвержден приказом ФСТЭК России от 09.02.2016 N 9. ДСП);
- «Требованиям безопасности информации к операционным системам» (утвержден приказом ФСТЭК России от 19.08.2016 N 119. ДСП);
- «Требования к средствам контроля съемных машинных носителей информации» (утвержден приказом ФСТЭК России от 28.07.2014 N 87. ДСП);
- Руководящий документ. Безопасность информационных технологий.
 Критерии оценки безопасности информационных технологий (введен в действие приказом Гостехкомиссии России от 19 июня 2002 г. N 187).

1.3. Наименование обладателя информации, заказчика, оператора систем и сетей

Обладателем информации, заказчиком и оператором систем и сетей является ООО «Вкусно и ладно».

1.4. Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей

Отдел службы защиты информации – администратор информационной безопасности.

Глава компании – генеральный директор.

1.5. Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии)

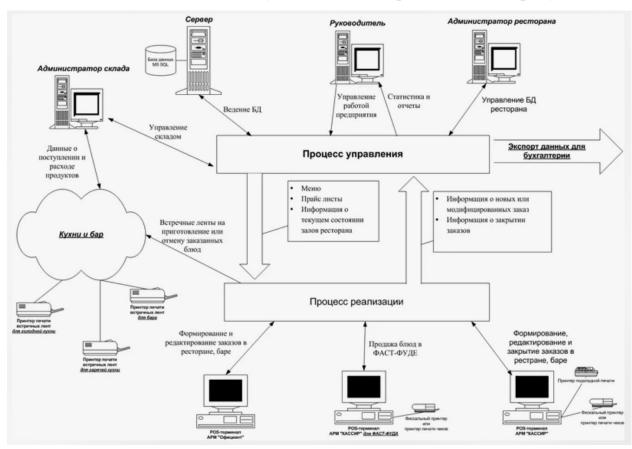
Разработка производилась силами ООО «Вкусно и Ладно».

2 Описание системами сетей и их характеристика как объектов зашиты

2.1. Наименование систем и сетей, для которых разработана модель угроз безопасности информации:

Наименование системы, для которой производится оценка угроз — Информационная система внутреннего и внешнего обмена ООО «Вкусно и Лално».

- объект 1 информационная система персональных данных ООО
 «Вкусно и Ладно»;
- объект 2 ЛВС, в рамках которой работники обеспечивают обмен информацией;
 - объект 3 сервер, на котором хранятся БД ПДн, «Вкусно и Ладно».
 Реализации сети ООО «Вкусно и Ладно» представлена на рисунке 1.



2.2. Нормативно правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети

Настоящая Политика разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее в тексте — Закон № 152-ФЗ), а также иными подзаконными нормативноправовыми актами в сфере персональных данных. И с учётом технического задания ПБ.

2.3. Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим; основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сети

Назначение: ИСПДн предназначена для обработки информации о заказчиках и пользователях, а также хранение всей информации на сервере.

ПДн обрабатываются с целью:

- предоставления услуг;
- обеспечивается защита от несанкционированного доступа на территорию посторонних лиц и транспортных средств;
- предоставление информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством.
 - обеспечение защиты прав и обязанностей работников;
 - осуществление трудовых договоров;
 - передача данных в уполномоченные органы (ФНС, ФСС, ПФР);
 - ведение расчетов заработной платы и надбавок;
 - осуществление банковских операций.

Правовые основание обработки персональных данных: Трудовой кодекс РФ, Налоговый кодекс, ФЗ «О бухгалтерском учете», лицензия на осуществление банковских операций, согласие на обработку персональных данных.

2.5. Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сети:

Обеспечение физической безопасности находящихся на объекте сотрудников и заказчиков, а также хранение, обработка и защита ПДн.

2.6. Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа в состав групп пользователей включается все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация)

Таблица 1 – Описание групп пользователей

Группа пользователей	Права пользователя		
Администратор безопасности	Пользователь с правами администратора безопасности		
Системный	Пользователь с правами администратора		
администратор	информационной системы		
Пользователь	Пользователь с правом наполнения информационной системы информацией, редактирования информации, и ее удаления.		

3 Виды тактик, применяемых нарушителем

- Т1 Сбор информации о системах и сетях
- Т2 Получение первоначального доступа к компонентам систем и сетей
- Т3 Внедрение и исполнение вредоносного программного обеспечения в системах и сетях
 - Т4 Закрепление (сохранение доступа) в системе или сети
- T5 Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ
 - Т6 Повышение привилегий по доступу к компонентам систем и сетей
- Т7 Сокрытие действий и применяемых при этом средств от обнаружения
- Т8 Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям
- Т9 Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз
- T10 Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям

Таблица 2 — Описание групп для внешних и внутренних нарушителей для объекта

Вид	Категория	Возможные цели	Уровень	Применяем	Гипотетичес
нарушите	возможно	реализации угроз	возможно	ые тактики	кая
ЛЯ	Γ0	безопасности	стей		актуальност
	нарушите	информации	нарушите		Ь
	ЛЯ		ЛЯ		
Отдельные физически е лица (хакеры)	Внешний	Получение финансовой или другой материальной выгоды.	H2	T1, T2, T3, T4, T5, T6, T7, T8, T9, T10	Актуально
Разработч ики программн ых, программн о-аппаратны х средств	й	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	Н3	T1, T2,T3,T4, T5, T6,T7,T8,T9, T10	Актуально
Лица, обеспечив ающие поставку программн ых, программн о- аппаратны х средств, обеспечив ающих систем	Внутренни й и внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	H2	T1, T2, T3,T4,T6,T10	Актуально
Лица, обеспечив ающие поставку программн ых,	Внутренни й и внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или	Н2	T1, T2, T3,T4,T6,T10	Актуально

		T .		<u> </u>	
программн		неквалифицированные			
O-		действия.			
аппаратны					
х средств,					
обеспечив					
ающих					
систем					
Лица,	Внутренни	Получение	H2	T1, T2,T3,T4,	Актуально
привлекае	й	финансовой или иной		T5 T6	
мые для		материальной выгоды.		T5, T6,	
установки,		Непреднамеренные,		T9,T10	
настройки,		неосторожные или			
испытаний		неквалифицированные			
,		действия.			
пусконала					
дочных и					
иных					
видов					
работ					
Лица,	Внутренни	Получение	H1	T1, T2,	Актуально
обеспечив	й	финансовой или иной		T2 T4 T6 T10	
ающие		материальной выгоды.		T3,T4,T6,T10	
функцион		Непреднамеренные,			
ирование		неосторожные или			
систем и		неквалифицированные			
сетей или		действия.			
обеспечив					
ающие					
системы					
оператора					
(админист					
рация,					
охрана,					
уборщики					
и т.д.)					

4. Возможные объекты воздействия угроз безопасности информации. Возможные негативные последствия реализации угроз безопасности информации. Источники угроз безопасности информации. Способы реализации угроз безопасности информации.

В отношении каждого объекта воздействия определялись виды воздействия на него, которые могут привести к негативным последствиям. Рассматриваемые виды воздействия представлены в Таблице 3.

Идентификатор	Вид воздействия
BB.1	Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)
BB.2	Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
BB.3	Отказ в обслуживании компонентов (нарушение доступности)
BB.4	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)
BB.5	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации

Способы реализации:

- СР.1 Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей)
 - СР.2 Внедрение вредоносного программного обеспечения
- СР.3 Использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств
- СР.4 Установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства
- СР.5 Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных
- СР.6 Реализация атак типа «отказ в обслуживании» в отношении технических средств, программного обеспечения и каналов передачи данных
- СР.7 Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации

СР.8 Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

СР.9 Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств

На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определен перечень рассматриваемых нарушителей, актуальных для систем и сетей. Данный перечень указан в Таблице 4.

реализации угроз безопасности информации возможных нарушителей Реализации угроз информации возможных нарушителей Реализации угроз безопасности информации информации предполагают наличие нарушителя Не имеют достаточной материальной выгоды. Получение финансовой или иной материальной выгоды. Не имеют достаточной информации, обрабатываемой в Подсистеме Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или иной материальной информации, обрабатываемой в Подсистеме Подсистеме Подривением деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме СР.3, СР.4, СР.7 СР.5 СР.5 СР.5 СР.5 СР.6 СР.6 СР.6 СР.6 СР.6 СР.6 СР.6 СР.6	Вид нарушителя	Возможные цели	Предположение об	Способы
Отдельные физические лица (хакеры) Конкурирующие организации Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Конкурирующие организации Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или иной материальной информации, обрабатываемой в подсистеме Подица, привлекаемые для Получение финансовой или иной материальной информации, обрабатываемой в подсистеме Получение финансовой или карактеристик безопасности конфиденциальной информации, обрабатываемой в подсистеме Подучение финансовой или карактеристик безопасности конфиденциальной информации, обрабатываемой в подсистеме Получение финансовой или карактеристик безопасности конфиденциальной информации, обрабатываемой в подсистеме Получение финансовой или карактериальной информации, обрабатываемой в подсистеме Получение финансовой или иной материальной или иной материальной или реализации угроз СР.1, СР.2, СР.2, СР.7, СР.3, СР.4, СР.7		реализации угроз	отнесении к числу	Реализации
физические лица (хакеры) иной материальной выгоды. Любопытство или желание самореализации. Конкурирующие организации Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или иной материальной информации, обрабатываемой в Подсистеме Поставщики Выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или неквалифицированные действия. Получение финансовой или неквалифицированные действия. Получение финансовой или неквалифицированные действия. Возможные цели реализации угроз СР.6 СР.7 СР.7, СР8 СР.7, СР8 Оср.1, СР.2, СР.2, СР.7, СР8 Оср.2, СР.7, СР8 Оср.3, СР.4, СР.7 СР.7 СР.7, СР8 Оср.4, СР.7 СР.7 СР.3, СР.4, СР.7 СР.7 СР.7 СР.7 СР.7 СР.6		безопасности информации	возможных нарушителей	
(хакеры) Выгоды. Любопытство или желание самореализации. Конкурирующие организации Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или иной материальной информации, обрабатываемой в подсистеме Поставщики выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или нереднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или неквалифицированные действия. Получение финансовой или нереднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или нереднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или ворабатываемой в подсистеме Подсистеме Получение финансовой или нереднамереные информации, обрабатываемой в подсистеме Подсистеме Получение финансовой или нереднамереные информации, обрабатываемой в подсистеме Получение финансовой или нереднамереные информации информаци информации информации информации информации информации информаци	Отдельные	Получение финансовой или	Возможные цели	CP.1, CP.2,
желание самореализации. Конкурирующие организации Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Поставщики вычислительных услуг, услуг связи неосторожные или неквалифицированные действия. Получение финансовой или не финансовой или неквалифицированные действия. Получение финансовой или ней материальной информации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или конфиденциальной информации, обрабатываемой в Подсистеме Подсистеме Получение финансовой или возможные цели реализации угроз СР.3, СР.4, СР.7	физические лица	иной материальной	реализации угроз	CP.6
Поставщики вычислительных услуг, услуг связи непосторожные или неквалифицированные действия. Получение финансовой или иной материальной выгоды. Поставщики вычислительных услуг, услуг связи непосторожные или неквалифицированные действия. Получение финансовой или ной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или ворабатываемой в подсистеме Подсистеме Получение финансовой или неквалифицированные действия. Получение финансовой или неквалифицированные действия. Возможные цели реализации угроз СР.3, СР.4, СР.7	(хакеры)	выгоды. Любопытство или	безопасности	
Конкурирующие организации Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Поставщики вычислительных услуг, услуг связи непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или необрабатываемой в подсистеме Подрабатываемой и поручения финансовой или неквалифицированные действия. Получение финансовой или неквалифицированные действия. Возможные цели реализации угроз СР.1, СР.2, СР.7, СР8 Отивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Подсистеме Получение финансовой или необрабатываемой в Подсистеме Получение финансовой или необрабатываемой в Подсистеме СР.3, СР.4, СР.7		желание самореализации.	информации	
Конкурирующие организации Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Не имеют достаточной осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Непреднамеренные действия. Непреднамеренные конфиденциальной информации, обрабатываемой в Подсистеме Поставщики вычислительных услуг, услуг связи безопасности конфиденциальной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Получение финансовой или вологистеме Получение финансовой или поряжение финансовой или поряжение цели реализации угроз СР.3, СР.4, СР.7			предполагают наличие	
организации преимуществ. Получение финансовой или иной материальной выгоды. Поставщики вычислительных услуг, услуг связи неосторожные или неквалифицированные действия. Получение финансовой или неквалифициальной информации, обрабатываемой в подсистеме Поставщики вычислительных услуг, услуг связи выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или неквалифицированные дели дележные цели дележные дележн			нарушителя	
финансовой или иной материальной выгоды. Финансовой или иной материальной выгоды. Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Подчение финансовой или неквалифицированные действия. Получение финансовой или неквалифицированные действия. Осуществления деятельности, связанной с нарушения деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Подсистеме Получение финансовой или возможные цели деятельности действия. Получение финансовой или возможные цели деятельности действия. Получение финансовой или неформации, обрабатываемой в подсистеме Подсистеме Получение финансовой или информации угроз СР.3, СР.4, СР.7	Конкурирующие	Получение конкурентных	Не имеют достаточной	CP.1, CP.2,
материальной выгоды. Деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Непреднамеренные, карактеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Лица, привлекаемые для иной материальной иной материальной иной материальной иной материальной иной материальной иной материальной иноформации, обрабатываемой в Подсистеме Получение финансовой или иной материальной иноформации угроз СР.3, СР.4, СР.7	организации	преимуществ. Получение	мотивации для	CP.7, CP8
Се нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или иной материальной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Получение финансовой или возможные цели реализации угроз СР.3, СР.4, СР.7		финансовой или иной	осуществления	
характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Подсистеме Получение финансовой или не имеют достаточной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Подучение финансовой или возможные цели СР.3, СР.4, привлекаемые для получение финансовой или реализации угроз СР.7		материальной выгоды.	деятельности, связанной	
безопасности конфиденциальной информации, обрабатываемой в Подсистеме Поставщики вычислительных услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Безопасности конфиденциальной информации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Получение финансовой или возможные цели реализации угроз СР.3, СР.4, СР.7			с нарушением	
Конфиденциальной информации, обрабатываемой в Подсистеме Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Непреднамеренные, неосторожные или неквалифицированные карактеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Получение финансовой или реализации угроз СР.3, СР.4, СР.7			* *	
Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Подчение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Подсистеме Подчение финансовой или выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Возможные цели реализации угроз СР.3, СР.4, СР.7				
Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Подеистеме Получение финансовой или иной материальной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Получение финансовой или привлекаемые для иной материальной реализации угроз Организации угроз СР.3, СР.4, СР.7				
Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или иной материальной вагоды. Непреднамеренные, неосторожные или неквалифицированные действия. Подсистеме Подсистеме СР.3, СР.4, СР.7 СР.7 СР.7				
Поставщики вычислительных услуг, услуг связи Непреднамеренные, неосторожные или неквалифицированные действия. Получение финансовой или иной материальной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Получение финансовой или привлекаемые для Получение финансовой или иной материальной иной материальной реализации угроз СР.3, СР.4, СР.7			_	
вычислительных услуг связи иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. СР.7 безопасности конфиденциальной информации, обрабатываемой в Подсистеме Лица, привлекаемые для иной материальной реализации угроз СР.7			Подсистеме	
услуг, услуг связи выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. безопасности конфиденциальной информации, обрабатываемой в Подсистеме Лица, привлекаемые для привлекаемые для выгоды. осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме СР.3, СР.4, реализации угроз СР.7	Поставщики	Получение финансовой или	Не имеют достаточной	CP.3, CP.4,
Непреднамеренные, неосторожные или неквалифицированные действия. Действия. Деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Лица, Получение финансовой или привлекаемые для иной материальной реализации угроз СР.3, СР.4, СР.7	вычислительных	иной материальной	мотивации для	CP.7
неосторожные или с нарушением карактеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Лица, Получение финансовой или привлекаемые для иной материальной реализации угроз СР.7	услуг, услуг связи	выгоды.	осуществления	
неквалифицированные действия. Карактеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме Лица, Получение финансовой или реализации угроз СР.7		Непреднамеренные,	деятельности, связанной	
действия. безопасности конфиденциальной информации, обрабатываемой в Подсистеме Лица, Получение финансовой или возможные цели реализации угроз СР.7		_	с нарушением	
конфиденциальной информации, обрабатываемой в Подсистеме Лица, Получение финансовой или реализации угроз СР.7			• •	
информации, обрабатываемой в Подсистеме Лица, Получение финансовой или возможные цели реализации угроз СР.7		действия.		
обрабатываемой в Подсистеме Лица, Получение финансовой или Возможные цели реализации угроз СР.7			конфиденциальной	
Подсистеме Лица, Получение финансовой или Возможные цели привлекаемые для иной материальной реализации угроз СР.7				
Лица, Получение финансовой или Возможные цели СР.3, СР.4, привлекаемые для иной материальной реализации угроз СР.7			•	
привлекаемые для иной материальной реализации угроз СР.7			Подсистеме	
	Лица,	Получение финансовой или	Возможные цели	CP.3, CP.4,
установки, выгоды. безопасности	привлекаемые для	иной материальной	реализации угроз	CP.7
· · · · · · · · · · · · · ·	установки,	выгоды.	безопасности	

Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположение об отнесении к числу возможных нарушителей	Способы Реализации
настройки, испытаний, пусконаладочных и иных видов работ	Непреднамеренные, неосторожные или неквалифицированные действия.	информации предполагают наличие нарушителя	
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.)	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	Не имеют достаточной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме.	CP.2, CP.7, CP.8
Авторизованные пользователи систем и сетей	Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя.	CP.1, CP.2, CP.6, CP.7, CP.8
Системные администраторы и администратор	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя	CP.1, CP.2, CP.4, CP.7, CP.8, CP.8, CP.9
Бывшие работники (пользователи)	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия.	Не имеют достаточной мотивации для осуществления деятельности.	CP.1, CP2, CP.8