МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ИКБ направление «Кибербразведка 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.

Москва 2023

Содержание

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 защиты

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

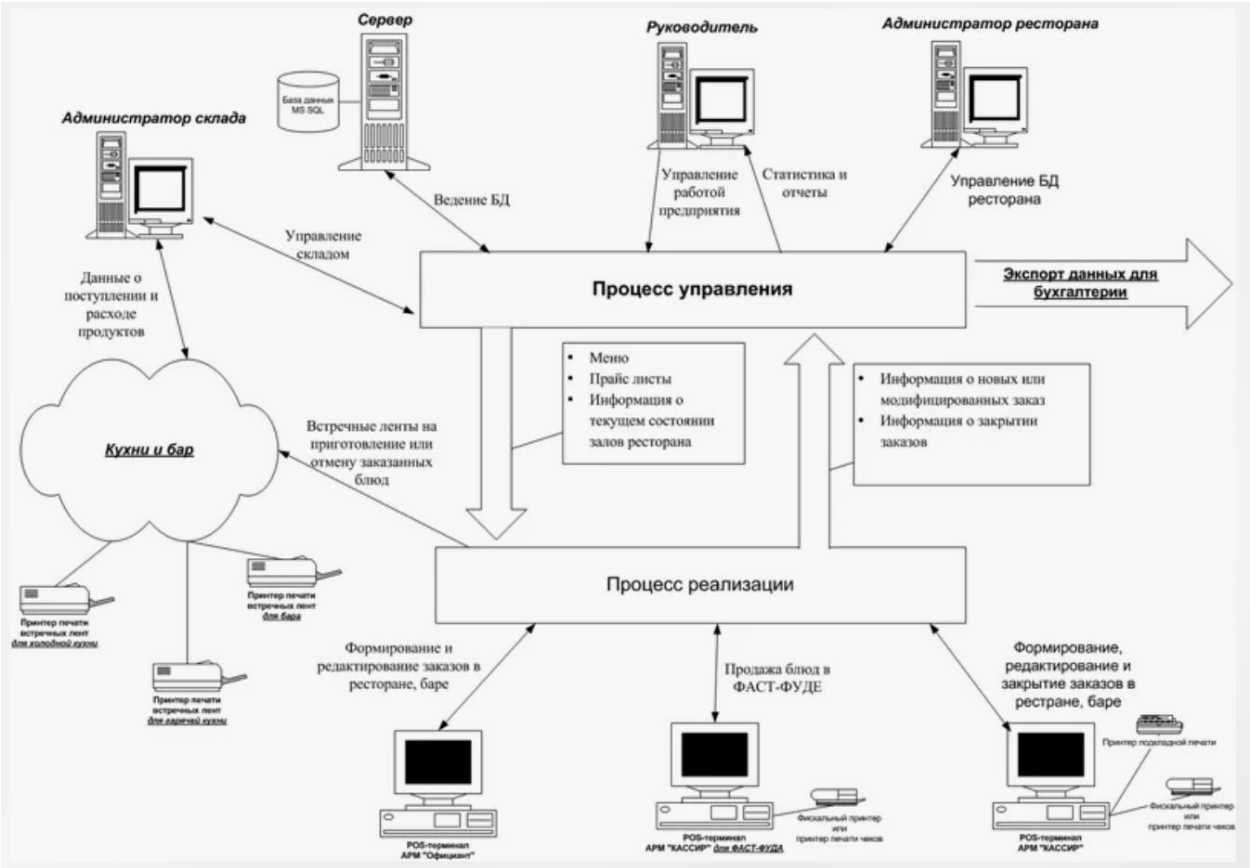
Наименование системы, для которой производится оценка угроз – Информационная система внутреннего и внешнего обмена ООО «Вкусно и Ладно».

– 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 нормативно-правовыми 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 администратор	Пользователь с правами администратора 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

Т5 - 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

Т10 - 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 нарушителя	**Категория возможного нарушителя**	**Возможные цели реализации угроз безопасности информации**	**Уровень возможностей нарушителя**	**Применяемые тактики**	**Гипотетическая актуальность**
Отдельные физические лица (хакеры)	Внешний	Получение финансовой или другой материальной выгоды.	H2	T1, T2,T3,T4, T5, T6,T7,T8, T9,T10	Актуально
Разработчики программных, программно-аппаратных средств	Внутренний	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	H3	T1, T2,T3,T4, T5, T6,T7,T8,T9, T10	Актуально
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внутренний и внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	H2	T1, T2, T3,T4,T6,T10	Актуально
Лица, обеспечивающие поставку программных,	Внутренний и внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или	H2	T1, T2, T3,T4,T6,T10	Актуально

программно-аппаратных средств, обеспечивающих систем		неквалифицированные действия.			
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	H2	T1, T2,T3,T4, T5, T6, T9,T10	Актуально
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	H1	T1, T2, T3,T4,T6,T10	Актуально

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
ВВ.1	Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)
ВВ.2	Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
ВВ.3	Отказ в обслуживании компонентов (нарушение доступности)
ВВ.4	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)
ВВ.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.

Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположение об отнесении к числу возможных нарушителей	Способы Реализации
Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя	СР.1, СР.2, СР.6
Конкурирующие организации	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды.	Не имеют достаточной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме	СР.1, СР.2, СР.7, СР8
Поставщики вычислительных услуг, услуг связи	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	СР.3, СР.4, СР.7
Лица, привлекаемые для установки,	Получение финансовой или иной материальной выгоды.	Возможные цели реализации угроз безопасности	СР.3, СР.4, СР.7

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.	СР.2, СР.7, СР.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.	СР.1, СР.2, СР.6, СР.7, СР.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	СР.1, СР.2, СР.4, СР.7, СР.8, СР.8, СР.9
Бывшие работники (пользователи)	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия.	Не имеют достаточной мотивации для осуществления деятельности.	СР.1, СР2, СР.8