УТВЕРЖДАЮ

Руководитель ООО «Регард»

_____/_____ /

«___» _____ 20__г.

Модель угроз безопасности информации в защищенной автоматизированной информационной системе ООО «Регард»

Общество с ограниченной ответственностью «Регард»

Москва 2023

Содержание

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИС	Автоматизированная информационная система
ПДн	Персональные данные
ИСПДн	Информационная система персональных данных
ЛВС	Локальная вычислительная сеть

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение Модели угроз

Разработка Модели угроз выполняется для определения актуальных угроз безопасности защищаемой информации, обрабатываемой в АИСПД ООО «Регард».

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

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 съёмных машинных носителей информации» (утвержден приказом ФСТЭК России от 28.07.2014 N 87. ДСП);

– Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (введён в действие приказом Гостехкомиссии России от 19 июня 2002 г. N 187).

1.3 Область применения настоящей Модели угроз

Областью применения процесса определения угроз безопасности информации является совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке информации в АИС ООО «Регард».

Элементами АИС ООО «Регард» являются:

– информация заказчика, как совокупность информации и её носителей, используемых в АИС ООО «Регард»;

– информационные технологии, применяемые при обработке информации;

– технологические средства, осуществляющие обработку информации (средства вычислительной техники, информационно-вычислительные комплексы сети, средства и системы хранения, передачи, приема и обработки информации);

– программные средства инфраструктурного уровня (в том числе операционные системы технических средств АИС ООО «Регард»);

– средства защиты информации;

– подсистемы и сервисы, образуемые на основе технических и программных средств, средства защиты информации АИС ООО «Регард» (в том числе инфраструктурные подсистемы, инфраструктурные сервисы, подсистемы информационной безопасности).

1.4 Наименование обладателя информации, заказчика, оператора систем и сетей

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

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

Ответственность за обеспечение защиты информации (безопасности) систем и сетей возлагается на руководителя подразделения информационной безопасности, администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

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

Отсутствует, разработка произведена собственными силами.

2 ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ

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

– объект 1 – информационная система персональных данных ООО «Регард»;

– объект 2 – ЛВС, в рамках которой работники обеспечивают обмен информацией;

– объект 3 – сервер, на котором хранятся БД ИСПДн, ООО «Регард».

2.2 Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных

Уровень защищенности ИСПДн ООО «Регард» – третий.

2.3 Нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети

Настоящая Модель угроз разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2.4 Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим

ИСПДн ООО «Регард» предназначены для обработки, хранения и защиты персональных данных сотрудников, клиентов, поставщиков и других физических лиц, связанных с деятельностью предприятия.

Основные задачи (функции) ИСПДн ООО «Регард»:

- сбор и хранение персональные данных, включая данные сотрудников, клиентов и других заинтересованных сторон;
- обеспечение контроля над доступом к персональным данным и информационным ресурсам в соответствии с уровнем доступа сотрудников;
- обработка персональных данных, включая обновление, анализ и создание отчетов на основе этих данных;

– обеспечение безопасности персональных данных, включая защиту от несанкционированного доступа, утечек и взломов;

– обеспечение соблюдения законодательства о защите персональных данных и других нормативных актов.

Состав обрабатываемой информации включает в себя персональные данные, такие как имена, даты рождения, адреса, номера паспортов, данные о трудоустройстве, налоговые и страховые данные, медицинская информация и другие данные, связанные с работой и взаимодействием сотрудников, клиентов и партнеров предприятия.

Правовой режим информации определяется законодательством о защите персональных данных и включает в себя требования к сбору, обработке, хранению и передаче персональных данных.

2.5 Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сеты

Такими процессами являются обеспечение физической безопасности находящихся на объекте сотрудников и хранение, обработка и защита персональных данных.

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

Типовая роль	Уровень доступа к ИСПДн	Разрешенные действия в ИСПДн
Сотрудники отдела информационной безопасности	Обладают полным функционалом для технической поддержки и для обслуживания информационных систем	расширенные полномочия для управления технической инфраструктурой
Администраторы систем и сетей	Обладает полной правами права на управление и настройку системы, полные права на настройку и конфигурацию системы, полный мониторинг и аудит системы, полное управление резервными копия и восстановлением данные	Полный доступ к управлению, настройкам и обслуживаниям информационных систем и сетей предприятия. полный доступ для администрирования.

Менеджеры и руководители	Обладают полномочиями для настройки и мониторинга безопасности данных.	Имеют доступ к данным и ресурсам, необходимым для принятия решений и управления бизнес-процессами
Отдел кадров	Доступ к данным сотрудников, включая информацию о трудоустройстве, заработной плате и другие данные.	Доступ к данным сотрудником, их персональные данные и т.п.
Разработчики	Имеют доступ к веб-сервисам для совместной разработки проектов, хранения кода	Просмотр, изменение и выполнения к данным и ресурсам сервисов для хранения кода
Специалисты по безопасности	Ответственные за обеспечение информационной безопасности и управление доступом.	Отслеживание различных активностей пользователей
Поставщики	Доступ к системам предприятия для взаимодействия в рамках поставок и заказов.	Просмотр заказов

2.7 Описание функционирования систем и сетей на базе информативно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры

Не реализовано.

2.8 Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателями информации, оператором и поставщиком вычислительных услуг

Не реализовано.

2.9 Описание условий использования информационно-телекоммуникационной инфраструктуры обработки данных или облачной инфраструктуры поставщика услуг (при наличии)

Не реализовано.

3 ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ.

Таблица 2 – Возможные цели реализации угроз безопасности информации нарушителями

№	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
1	Отдельные физические лица (хакеры)	Внешний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)
2	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
3	Авторизованные пользователи систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
4	Системные администраторы и администраторы безопасности	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия

Таблица 3 – Описание групп пользователей

Негативные последствия	Объекты воздействия	Виды воздействия
Потеря (хищение) данных	Серверы и хранилища данных	Несанкционированная подмена данных, содержащихся на серверах

	АРМы бухгалтерии	Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации на АРМ главного бухгалтера
	АРМы финансового департамента	Подмена данных, переделанная информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора
Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса	АРМы отдела Информационной безопасности	Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации
	АРМ главного инженера/администратора	Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и (или) к изменению логики ПЛК
Недоступность данных	Серверы и хранилища данных	Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты
	Программное обеспечение	Несанкционированная отправка команд, приводящая к остановке бизнес процессов
	Сетевая инфраструктура	Несанкционированная модификация (изменение) логики работы или установок коммутационного контроллера, которая приводит к остановке бизнес-процессов
Утечка персональных данных	Серверы и хранилища данных	Нарушение безопасности может привести к утечке персональных данных, что может вызвать ущерб репутации предприятия и привести к юридическим последствиям.

Таблица 4 – Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

Виды нарушителей	**Возможные цели реализации угроз безопасности информации**			**Соответствие целей видам риска (ущерба) и возможным негативным последствиям**
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству	

Отдельные физические лица (хакеры)	Желание самореализоваться	Получение финансовой выгоды за счет кражи и коммерческой тайны	-	Нарушение личной, семейной тайны, утрата чести и доброго имени; утечка коммерческой тайны; потеря клиентов
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Передача информации о физическом лице третьим лицам	Передача информации о физическом/юридическом лице третьим лицам, а также о структуре внутренней системы	-	Нарушение функционирования
Авторизованные пользователи систем и сетей	Непреднамеренные, неосторожные или неквалифицированные действия	-	-	Финансовый, иной материальный ущерб физическим лицам
Системные администраторы и администраторы безопасности	Месть за ранее совершенные действия	Любопытство или желание самореализации	Получение финансовой или иной материальной выгоды при вступлении в сговор с преступной группой	Финансовый, иной материальный ущерб физическим лицам; невозможность заключения договоров, соглашений; утечка информации ограниченного доступа

4 СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Таблица 5 – Сценарии реализации угроз безопасности информации

Нарушитель	**Категория нарушителя**	**Объект воздействия**	**Негативные последствия**	**Способ реализации**	**Актуальные тактики для реализации УБИ**
Отдельные физические лица (хакеры)	Внешний	Телекоммуникационное оборудование	НП1, НП4	СР.1, СР.2, СР.10, СР.7	Т.1.5, Т1.11, Т2.4, Т2.5
		Информация (данные), содержащаяся в системах и сетях	НП1, НП6	СР.8	Т.1.5, Т1.11, Т2.4, Т2.5
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний / Внешний	Программно-аппаратные средства обработки и хранения информации (ПЭВМ, сервера)	НП3, НП4, НП5	СР.1, СР.2, СР.3, СР.6, СР.7, СР.9	Т2.9, Т10.1, Т10.10
Авторизованные пользователи систем и сетей	Внутренний	Информация (данные), содержащаяся в системах и сетях	НП1, НП4	СР.1, СР.3, СР.5, СР.7, СР.9	Т2.7, Т2.9, Т8.4
Системные администраторы и администраторы безопасности	Внутренний	Программно-аппаратные средства обработки и хранения информации (ПЭВМ, сервера)	НП3, НП4, НП5, НП6	СР.1, СР.2, СР.6, СР.7, СР.9	Т2.4, Т2.5, Т2.9, Т10.10, Т10.11

5 АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИ

Таблица 6 – Показатели исходной защищенности ИСПДн ООО «Регард»

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:		+	
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	–
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	–
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	–	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная ИСПДн, развернутая в пределах одного здания	–	–	–
2. По наличию соединения с сетями общего пользования:		+	
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	–
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	–	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			+
чтение, поиск;	–	–	+
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4.По разграничению доступа к персональным данным:		+	
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	–	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	+	–
ИСПДн с открытым доступом	–	–	–
5. По наличию соединений с другими базами ПДн иных ИСПДн:		+	
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	+	–

ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	–	–	–
6. По уровню обобщения (обезличивания) ПДн:			+
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	–	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	–	+
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	–
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:	+		
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	–
ИСПДн, предоставляющая часть ПДн;	–	–	–
ИСПДн, не предоставляющая никакой информации.	+	–	–

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

По результатам, ИСПДн ООО «Регард» соответствует среднему уровню защищенности.