УТВЕРЖДАЮ

Руководитель

_____

«___» _____ 202_г.

Модель угроз безопасности информации защищённой автоматизированной информационной системы ООО «ГК Иннохет»

г. Москва

2023 г.

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИС – Автоматизированная информационная система

БД – База данных

ИСПДн – Информационная система персональных данных

ФГБУ – Федеральное государственное бюджетное учреждение

НИЦ – Национальный исследовательский центр

НСД – Несанкционированный доступ

ОС – Операционная система

ПДн – Персональные данные

ПО – Программное обеспечение

ЛВС – Локально вычислительная сеть

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение и область модели угроз

Разработка модели угроз безопасности информации выполняется для определения актуальных угроз безопасности защищаемой информации, обрабатываемой в ООО «ГК Иннохет» Сама компания является высокотехнологичной быстроразвивающаяся компанией, создающая инновационные решения для цифровизации банковской отрасли.

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

1.2 Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз

Определение нарушителей и угроз безопасности персональных данных при их обработке и последующее формирование на их основе модели угроз и нарушителей является одним из необходимых мероприятий по обеспечению безопасности в информационных системах:

– 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»;

– 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»;

− Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне»;

– 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»;

– Федеральный закон от 02.12.1990 N 395-1 ФЗ-395-1 «О Банках и банковской деятельности»

– Приказ ФСТЭК России от 16 июня 2023 г N 118 «Требования по безопасности информации к средствам контейнеризации»

1.3 Наименование обладателя информации, заказчика, оператора систем и сетей

Заказчиком и оператором систем и сетей является ООО «ГК Иннохет»

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

Департаменты, отвечающие за обеспечение безопасности информации выступают:

- Руководитель направления дивизона ИБ. В задачи данного дивизиона входит обслуживание и администрирование средств информационной безопасности.

- Отдел информационной безопасности (ИБ). В задачи данного департамента входит анализирование средств информационной безопасности.

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

Отсутствует

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 «ГК Иннотех»

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

– объект 3 – сервер, на котором хранятся БД ИСПДн, ООО «ГК ИННОТЕХ»

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

Класс защищенности: Класс защищенности систем и сетей определяет уровень и глубину мер безопасности, которые должны быть применены к информационным ресурсам. В России классы защищенности могут определяться согласно ГОСТ Р ИСО/МЭК 27001-2012 и другим нормативам.

Обычно они имеют следующие обозначения:

- КС1 (критический класс защищенности).
- КС2 (высокий класс защищенности).
- КС3 (средний класс защищенности).
- КС4 (низкий класс защищенности).

Уровень защищенности ИСПДн ООО «ГК ИННОТЕХ» - КС2

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

В ИСПДн ООО «ГК ИННОТЕХ» могут обрабатываться следующие персональные данные:

Основные задачи ИСПДн ООО «ГК ИННОТЕХ»

– разработка и тестирование безопасности объектов микросервисной архитектуры

– обеспечение информационной безопасности объектов интеллектуальной собственности организации

– обеспечение безопасности ПД, включая защиты от НСД, утечек и взломов

– передачи данных в уполномоченные органы (ФНС, ФСС, ПФР);

– ведения расчётов заработной платы и надбавок;

– осуществления банковских операций.

Состав обрабатываемой информации включает в себя персональные данные: имена, даты рождения, номер паспорта, данные о трудоустройстве

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

Контрагент ООО «ГК ИННОТЕХ» должен регулярно проводить следующие процессы для обеспечения безопасности:

- Сбор событий информационной безопасности;
- Управление доступом
- Обучение сотрудников**;**
- Реагирование на инциденты информационной безопасности;
- Соблюдение законодательства РФ.

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 к ИСПДн**
Администраторы систем и сетей	Обладают полной информацией о системном и прикладном программном обеспечении	Полный доступ к управлению, настройкам и обслуживаниям информационных систем и сетей предприятия. полный доступ для администрирования
Менеджеры и руководители	Обладают частичными доступами для настройки и мониторинга безопасности данных	Имеют частичный доступ к данным и ресурсам для управления бизнес-процессами.
Разработчики	Имеют доступ к веб-сервисам для совместной разработки проектов, хранения кода	Просмотр, изменение и выполнения к данным и ресурсам сервисов для хранения кода
Отдел SAST, DAST, CA	Имеют доступ к веб-сервисам для совместной разработки проектов, хранения кода	Просмотр, изменение и выполнения к данным и ресурсам сервисов для хранения кода, образов Docker – для тестирования безопасности компонентов
Отдел кадров	Имеют доступ к персональным данным сотрудников, включая информацию о заработной плане	Доступ к персональным данным сотрудников
Финансовый отдел (бухгалтерия)	Обладают доступом к бухгалтерской информации, финансовым данным.	Доступ к отчетам, договорам компании
Специалисты информационной безопасности	Контроль событий ИБ и контроль доступа	Уточнение, использование

Заказчики	Отсутствует	Предоставление Пдн

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. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОТИ ИНФОРМАЦИИ

Таблица 3 – Возможные цели реализации угроз безопасности информации нарушителями

вида	**Виды нарушителя**	**Категории нарушителя**	**Возможные цели реализации угроз безопасности информации**
1	Отдельные физические лица (хакеры)	**Внешний**	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
2	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
3	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 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 в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**	
Отдельные физические лица (хакеры)	+	+	**+ (получение финансовой или иной материальной выгоды при вступлении в сговор с преступной группой)**	**У1 (финансовый, иной материальный ущерб физическим лицам) У2**

				(невозможность заключения договоров, соглашений) **У3** **(утечка информации ограниченного доступа**
Авторизованные пользователи систем и сетей	+ **(непреднамеренные, неосторожные или неквалифицированные действия)**	-	-	**У1** **(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)**	**У1** **(финансовый, иной материальный ущерб физическим лицам)** **У2** **(невозможность заключения договоров, соглашений)** **У3** **(утечка информации ограниченного доступа**

4. СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ

Таблица 5 – Определение актуальных способов реализации угроз безопасности информации.

N п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Отдельные физические лица (хакеры)	**Внешний**	Удаленное автоматизированное рабочее место (АРМ) пользователя: несанкционированный доступ к операционной системе АРМ пользователя; нарушение конфиденциальности информации, содержащейся на АРМ пользователя	Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базами данных
			Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных: перехват (нарушение конфиденциальности) защищаемой информации,	Канал передачи данных между сервером основного центра обработки данных и сервером резервного центра обработки данных	Установка программных закладок в телекоммуникационное оборудование

N п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
2	Авторизованные пользователи систем и сетей (Н1)	**Внутренний**	АРМ главного бухгалтера организации: модификация платежных поручений, хранящихся на АРМ главного бухгалтера	Локальная вычислительная сеть организации	Ошибочные действия в ходе настройки АРМ главного бухгалтера
			Сервер базы данных веб-сайта портала государственных услуг (сервисов): отказ в обслуживании отдельных компонентов или систем и сетей в целом	Веб-интерфейс системы администрирования веб-сайта портала государственных услуг	Нарушение цепочки услуг по администрированию портала государственных усл

5. АКТУАЛЬНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если, то возможность реализации угрозы признается низкой;

если, то возможность реализации угрозы признается средней;

если, то возможность реализации угрозы признается высокой;

если, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

При составлении перечня актуальных угроз безопасности персональных данных каждой степени исходного уровня защищенности ИСПДн ставится в соответствие числовой коэффициент Y_1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности

Таблица 6 – Правила отнесения угрозы безопасности ПДн к актуальной

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности			
		Высокий	Средний	Низкий
Итого		∑>70%	∑ <30%	0%

Таблица 7 – Показатель исходного уровня защищенности ИСПДн

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 персональных данных;			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	+	-	-
ИСПДн с открытым доступом	-	+	-
5. По наличию соединений с другими базами персональных данных иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз персональных данных ИСПДн, при этом организация не является владельцем всех используемых баз персональных данных);	-	+	-
ИСПДн, в которой используется одна база персональных данных, принадлежащая организации – владельцу данной ИСПДн	+	-	-
6. По уровню обобщения (обезличивания) персональных данных:			
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 персональных данных)	+	-	-
7. По объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с персональными данными;	-	-	+
ИСПДн, предоставляющая часть персональных данных;	-	+	-

ИСПДн, не предоставляющая никакой информации.	+	-	-
Итого	∑ = 7 (70%)	∑ = 2 (20.%)	∑ = 1(10%)
	∑ ≥ 70 %		

ИСПДн имеет высокий уровень защищенности