УТВЕРЖДАЮ:

ООО «ХК «Авангард»

Директор по информационным технологиям

Ефимов Андрей Владимирович

подпись Ф.И.О.

«23» 01 2023 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Выполнение работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и оказание услуги по авторскому надзору за созданием системы защиты персональных данных для ООО "ХК "Авангард"

1. ПРЕДМЕТ ЗАКУПКИ:

Выполнение работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и оказание услуги по авторскому надзору за созданием системы защиты персональных данных для ООО "ХК "Авангард".

2. МЕСТО ВЫПОЛНЕНИЯ РАБОТ И ОКАЗАНИЯ УСЛУГ:

Место выполнения работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и оказание услуги по авторскому надзору за созданием системы защиты персональных данных для ООО "ХК "Авангард" - по месту осуществления деятельности Подрядчика.

3. СРОК И УСЛОВИЯ ВЫПОЛНЕНИЯ РАБОТ/ОКАЗАНИЯ УСЛУГ:

Срок выполнения работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации: не более 65 календарных дней с даты подписания договора.

Этапность и состав выполняемых работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации:

- Этап 1. Формирование требований к защите информации, содержащейся в информационных системах, где осуществляется обработка персональных данных;
- Этап 2. Разработка технического задания на создание системы защиты персональных данных;
- Этап 3. Разработка организационно-распорядительной документации и анализ защищенности информационных систем, где осуществляется обработка персональных данных;
- Этап 4. Оценка соответствия реализованных мер защиты персональных данных для информационных систем, где осуществляется обработка персональных данных.

Сроки завершения отдельных этапов работ определяются Подрядчиком самостоятельно при соблюдении условия – конечный срок выполнения работ по всем этапам составляет не более 65 календарных дней с даты подписания договора.
Период, в котором Подрядчик должен оказать разовую услугу по авторскому надзору за созданием системы защиты персональных данных по запросу от Заказчика - составляет 8 месяцев с момента подписания акта сдачи-приёмки всех этапов выполненных работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации.

Этапность и состав услуги по авторскому надзору за созданием системы защиты персональных данных:

- Этап 1. Анализ защищенности информационных систем, где осуществляется обработка персональных данных (повторные мероприятия);
- Этап 2. Оценка соответствия реализованных мер защиты персональных данных для информационных систем, где осуществляется обработка персональных данных (повторные мероприятия).

Оценка соответствия реализованных мер защиты персональных данных должна быть выполнена в соответствии с программой и методиками оценки соответствия реализованных мер защиты персональных данных, разработанной Подрядчиком и согласованной Заказчиком на моменте выполнения работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации.

Программа и методики проведения оценки соответствия могут быть уточнены и скорректированы по согласованию с Заказчиком в ходе самой оценки.

По результатам проведения повторных мероприятий Подрядчиком оформляется заключение, содержащее оценку соответствия информационных систем, где осуществляется обработка персональных данных (Приложение №2 к Техническому заданию), требованиям по защите персональных данных.

Срок выполнения этапов оказания услуги по авторскому надзору за созданием системы защиты персональных данных – не более 30 календарных дней со дня получения Подрядчиком уведомления от Заказчика по электронной почте.

Сроки завершения отдельных этапов оказания услуги определяются Подрядчиком самостоятельно при соблюдении условия – конечный срок по всем этапам оказания услуги составляет не более 30 календарных дней со дня получения Подрядчиком уведомления по электронной почте.

4. УСЛОВИЯ ОПЛАТЫ ВЫПОЛНЕНИЯ РАБОТ И ОКАЗАНИЯ УСЛУГ:

Оплата работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации путем безналичного перечисления денежных средств на расчетный счет Подрядчика в течение 10 банковских дней с даты подписания Заказчиком акта сдачи-приемки всех этапов выполненных работ на основании выставленного Подрядчиком счета.

Оплата услуги по авторскому надзору за созданием системы защиты персональных данных путем безналичного перечисления денежных средств на расчетный счет

Подрядчика в течение 10 банковских дней с даты подписания Заказчиком акта сдачи-приемки всех этапов услуги на основании выставленного Подрядчиком счета.

5. ПЕРИОД ФИКСАЦИИ ЦЕН:

Цены на работы по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и услуги по авторскому надзору за созданием системы защиты персональных данных фиксируются на весь срок действия Договора.

6. СРОК ДЕЙСТВИЯ ДОГОВОРА:

Договор вступает в силу с момента его подписания обеими Сторонами и действует до полного исполнения обязательств Сторонами по настоящему Договору.

7. ТРЕБОВАНИЯ К СОСТАВУ РАБОТ/УСЛУГ:

Выполнение работ/оказание услуги в соответствие с Приложениями к настоящему Техническому заданию 1–3:

Приложение №1 «Перечень персональных данных, которые обрабатываются в информационных системах, включенных в границы работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации»;

Приложение №2 «Перечень информационных систем, включенных в границы работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и оказанию услуги по авторскому надзору за созданием системы защиты персональных данных»;

Приложение №3 «Пояснительная записка к Техническому Заданию на выполнение работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и оказанию услуги по авторскому надзору за созданием системы защиты персональных для ООО "ХК "Авангард"».

В состав работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации должны входить этапы:

- Этап 1. Формирование требований к защите информации, содержащейся в информационных системах, где осуществляется обработка персональных данных;
- Этап 2. Разработка технического задания на создание системы защиты персональных данных;
- Этап 3. Разработка организационно-распорядительной документации и анализ защищенности информационных систем, где осуществляется обработка персональных данных;
- Этап 4. Оценка соответствия реализованных мер защиты персональных данных для информационных систем, где осуществляется обработка персональных данных.

В состав услуги по авторскому надзору за созданием системы защиты персональных данных должны входить следующие этапы:

- Этап 1. Анализ защищенности информационных систем, где осуществляется обработка персональных данных (повторные мероприятия);
- Этап 2. Оценка соответствия реализованных мер защиты персональных данных для информационных систем, где осуществляется обработка персональных данных (повторные мероприятия).

8. ОБЯЗАТЕЛЬНЫЕ ТРЕБОВАНИЯ К ПРЕТЕНДЕНТАМ:

1. Подрядчик должен иметь действующую лицензию Федеральной службы по техническому и экспортному контролю России на деятельность по технической защите конфиденциальной информации, со следующими разрешенными видами работ, услуг, составляющими лицензируемый вид деятельности (в соответствии с пунктом 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. №79):
   - б - услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
   - г - работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации (г1 - средств и систем информатизации);
   - д - работы и услуги по проектированию в защищенном исполнении (д1 - средств и систем информатизации);
   - е - услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации:
     - е4 - программных (программно-технических) средств защиты информации;
     - е5 - защищенных программных (программно-технических) средств обработки информации;
     - е6 - программных (программно-технических) средств контроля эффективности защиты информации).
2. Подрядчик должен иметь опыт реализации проектов по тематике работ (подтверждается документально) за последние 3 (три) года, в количестве не менее 5 проектов.
3. Возраст организации Подрядчика – не менее 3 (трёх) лет.

9. КРИТЕРИИ ОЦЕНКИ:

Стоимость предложения.

Приложения к Техническому заданию:

1. Перечень персональных данных, которые обрабатываются в информационных системах, включенных в границы работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации;
2. Перечень информационных систем, включенных в границы работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и оказанию услуги по авторскому надзору за созданием системы защиты персональных данных;
3. Пояснительная записка к Техническому Заданию на выполнение работ по приведению процессов обработки и защиты персональных данных в

соответствие требованиям законодательства Российской Федерации и оказанию услуги по авторскому надзору за созданием системы защиты персональных для ООО "ХК "Авангард".

Исполнитель:_____ /Рецлав Н.Н.

СОГЛАСОВАНО:

Директор по корпоративной защите_____ /Подорожкин В.Ю./

Руководитель направления ИТ-сервисов_____ /Закиров Д.Р./

Приложение №1
К Техническому заданию

Перечень персональных данных, которые обрабатываются в информационных системах, включенных в границы работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации

№	Состав обрабатываемых персональных данных
1.	Фамилия, имя, отчество
2.	Фотография
3.	Дата рождения
4.	Пол
5.	Адрес (город и район)
6.	Телефонный номер мобильный
7.	Номер карты Лояльности
8.	Адрес электронной почты
9.	Сведения о семейном положении
10.	Сведения о составе семьи – наличие детей

Исполнитель:_____ /Рецлав Н.Н.

СОГЛАСОВАНО:

Директор по корпоративной защите_____ /Подорожкин В.Ю./

Руководитель направления ИТ-сервисов_____ /Закиров Д.Р./

Приложение №2
К Техническому заданию

Перечень информационных систем, включенных в границы работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и оказанию услуги по авторскому надзору за созданием системы защиты персональных данных

№	Наименование ИС	Назначение ИС	Тип информации	Объем персональных данных в ИС	Примерное количество АРМ пользователей		Примерное количество серверов ИС		На каких площадках размещаются компоненты ИС	
					Физических	Виртуальных (версия VDI)	Физических	Виртуальных (версия гипервизора)	АРМ	Серверы
1.	1С:Управление Торговлей	Ведение розничной торговли и складского учета мерча	персональные данные клиентов	Более 100000 клиентов	50	0	0	4 (VMware)	644119, г. Омск, ул. Лукашевича, д. 35; 644024, г. Омск, ул. Ленина д. 20	127410, г. Москва, Алтуфьевское ш., д. 33Г
2.	R-keeper	Комплексная автоматизация общественного питания	персональные данные клиентов	Более 100000 клиентов	106	0	0	3 (VMware)	644119, г. Омск, ул. Лукашевича, д. 35; 644024, г. Омск, ул. Ленина д. 20	127410, г. Москва, Алтуфьевское ш., д. 33Г
3.	CRM B2C (текущая) / Программа лояльности (текущая)	Автоматизация продаж и маркетинг	персональные данные клиентов	Более 100000 клиентов	22	0	0	2 (VMware)	644119, г. Омск, ул. Лукашевича, д. 35;	125412, г. Москва, Коровинское шоссе 41
4.	CRM B2C (новая)	Автоматизация продаж и маркетинг	персональные данные клиентов	Более 100000 клиентов	22	0	0	1 (VMware)	644119, г. Омск, ул. Лукашевича, д. 35;	127410, г. Москва, Алтуфьевское ш., д. 33Г
5.	CRM B2B (новая)	Система управления мероприятиями и спонсорами	Нет данных	Нет данных	22	0	0	1 (VMware)	644119, г. Омск, ул. Лукашевича, д. 35;	127410, г. Москва, Алтуфьевское ш., д. 33Г

№	Наименование ИС	Назначение ИС	Тип информации	Объем персональных данных в ИС	Примерное количество АРМ пользователей		Примерное количество серверов ИС		На каких площадках размещаются компоненты ИС	
					Физических	Виртуальных (версия VDI)	Физических	Виртуальных (версия гипервизора)	АРМ	Серверы
6.	Клиентский сервис (новая)	Сервис личного кабинета (новый)	персональные данные клиентов	Более 100000 клиентов	22	0	0	1 (VMware)	644119, г. Омск, ул. Лукашевича, д. 35;	127410, г. Москва, Алтуфьевское ш., д. 33Г
7.	Программа лояльности (новая)	Система материальных и нематериальных вознаграждений	персональные данные клиентов	Более 100000 клиентов	22	0	0	1 (VMware)	644119, г. Омск, ул. Лукашевича, д. 35;	127410, г. Москва, Алтуфьевское ш., д. 33Г
8.	Сайт Программы лояльность loyalty.hawk.ru (текущий)	Регистрация в программе лояльности	персональные данные клиентов	Более 100000 клиентов	22	0	0	1 (VMware)	644119, г. Омск, ул. Лукашевича, д. 35;	125412, г. Москва, Коровинское шоссе 41
9.	Биометрическая система распознавания лиц «Визирь»	Система видео-идентификации физических лиц	персональные данные лиц, которым запрещено посещение мест проведения официальных спортивных соревнований	нет данных.	2	0	15	0	644119, г. Омск, ул. Лукашевича, д. 35;	644119, г. Омск, ул. Лукашевича, д. 35;
10.	Сайт - магазин shop.hawk.ru	Автоматизация розничной продажи мерча	персональные данные клиентов	Более 100000 клиентов	22	0	0	4 (VMware)	644119, г. Омск, ул. Лукашевича, д. 35;	125412, г. Москва, Коровинское шоссе 41
11.	Сайт сервиса «Личный кабинет» my.hawk.ru	Сервис личного кабинета. Единая авторизация	персональные данные клиентов	Нет данных	Нет данных	0	0	6	Нет данных	125412, г. Москва, Коровинское шоссе 41

№	Наименование ИС	Назначение ИС	Тип информации	Объем персональных данных в ИС	Примерное количество АРМ пользователей		Примерное количество серверов ИС		На каких площадках размещаются компоненты ИС	
					Физических	Виртуальных (версия VDI)	Физических	Виртуальных (версия гипервизора)	АРМ	Серверы
		для веб-сервисов ХК Авангард								
12.	Билетная система tickets.hawk.ru	Автоматизация продаж билетов на мероприятия спорткомплекса Gdrive-арена	персональные данные клиентов	Более 100000 клиентов	12	0	1	5 (VMware)	644119, г. Омск, ул. Лукашевича, д. 35; 644008, г. Омск, пр. Мира, д. 1Б	125412, г. Москва, Коровинское шоссе 41 644008, г. Омск, пр. Мира, д. 1Б
13.	Система терминального доступа	Удаленный доступ к инфраструктуре ХК Авангард	персональные данные клиентов	Более 100000 клиентов	Количество лицензий терминального доступа 50 шт.	0	0	4 (VMware)	Нет данных	127410, г. Москва, Алтуфьевское ш., д. 33Г

Исполнитель:_____ /Рецлав Н.Н.

СОГЛАСОВАНО:

Директор по корпоративной защите_____ /Подорожкин В.Ю./

Руководитель направления ИТ-сервисов_____ /Закиров Д.Р./

Приложение №3
К Техническому заданию

Пояснительная записка к Техническому Заданию на выполнение работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и оказанию услуги по авторскому надзору за созданием системы защиты персональных для ООО "ХК "Авангард"

Исполнитель:_____ /Рецлав Н.Н.

СОГЛАСОВАНО:

Директор по корпоративной защите_____ /Подорожкин В.Ю./

Руководитель направления ИТ-сервисов_____ /Закиров Д.Р./

(подпись)

Содержание

Обозначения и сокращения

№ п/п	Сокращение	Расшифровка сокращения
1.	ЗИ	Защита информации
2.	ИБ	Информационная безопасность
3.	ИС	Информационная система
4.	ИСПДн	Информационная система персональных данных
5.	ЛВС	Локальная вычислительная сеть
6.	ОРД	Организационно-распорядительная документация
7.	ПО	Программное обеспечение
8.	РФ	Российская Федерация
9.	СЗПДн	Система защиты персональных данных
10.	СрЗИ	Средство защиты информации
11.	СУБД	Система управления базами данных
12.	ТЗ	Техническое задание
13.	ФЗ	Федеральный закон
14.	ФСБ России	Федеральная служба безопасности Российской Федерации
15.	ФСТЭК России	Федеральная служба по техническому и экспортному контролю

1 Общие сведения

1.1 Наименование работ и услуг

Работы по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и услуга по авторскому надзору по созданию системы защиты персональных данных для ООО "ХК "Авангард".

1.2 Цели и задачи выполнения работ и оказания услуг

Целью выполнения работ и оказания услуги является обеспечение защиты ПДн, обрабатываемых Заказчиком, в соответствие с требованиями законодательства Российской Федерации по ПДн.

Для достижения поставленной цели необходимо решить следующие задачи:

- осуществить сбор и анализ исходных данных об информационных системах персональных данных (далее – ИСПДн) Заказчика и о применяемых Заказчиком мерах и способах защиты ПДн;
- проанализировать внутренние документы Заказчика, регламентирующие обеспечение информационной безопасности;
- провести анализ угроз безопасности ПДн и разработать модель угроз и модель нарушителей;
- определить необходимые уровни защищенности ПДн при их обработке в ИСПДн Заказчика;
- оценить соответствие текущего состояния защищенности ПДн требованиям законодательства;
- разработать предложения по внесению изменений в процессы обработки ПДн, а также разработать рекомендации по достижению уровня соответствия требованиям законодательства по ПДн;
- определить требования к системе защиты персональных данных (далее – СЗПДн);
- разработать техническое задание на создание СЗПДн;
- актуализировать организационно-распорядительную документацию в соответствии с требованиями законодательства РФ по обработке и защите ПДн;
- провести оценку соответствия реализованных мер защиты ПДн.

1.3 Наименования организации Заказчика

Организация Заказчик (далее – Заказчик): Общество с ограниченной ответственностью «Хоккейный клуб Авангард» (ООО «ХК Авангард»), 644010, г. Омск, ул. Куйбышева, 132, корп. 3, пом.89.

1.4 Сроки выполнения работ и оказания услуг

Срок выполнения работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации: не более 65 календарных дней с даты подписания договора.

Этапность и состав выполняемых работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации:

- Этап 1. Формирование требований к защите информации, содержащейся в информационных системах, где осуществляется обработка персональных данных;
- Этап 2. Разработка технического задания на создание системы защиты персональных данных;
- Этап 3. Разработка организационно-распорядительной документации и анализ защищенности информационных систем, где осуществляется обработка персональных данных;
- Этап 4. Оценка соответствия реализованных мер защиты персональных данных для информационных систем, где осуществляется обработка персональных данных.

Сроки завершения отдельных этапов работ определяются Подрядчиком самостоятельно при соблюдении условия – конечный срок выполнения работ по всем этапам составляет не более 65 календарных дней с даты подписания договора.

Период, в котором Подрядчик должен оказать разовую услугу по авторскому надзору за созданием системы защиты персональных данных по запросу от Заказчика - составляет 8 месяцев с момента подписания акта сдачи-приёмки всех этапов выполненных работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации.

Этапность и состав услуги по авторскому надзору за созданием системы защиты персональных данных:

- Этап 1. Анализ защищенности информационных систем, где осуществляется обработка персональных данных (повторные мероприятия);
- Этап 2. Оценка соответствия реализованных мер защиты персональных данных для информационных систем, где осуществляется обработка персональных данных (повторные мероприятия).

Срок выполнения этапов оказания услуги по авторскому надзору за созданием системы защиты персональных данных – не более 30 календарных дней со дня получения Подрядчиком уведомления от Заказчика по электронной почте.

Сроки завершения отдельных этапов оказания услуги определяются Подрядчиком самостоятельно при соблюдении условия – конечный срок по всем этапам оказания услуги составляет не более 30 календарных дней со дня получения Подрядчиком уведомления по электронной почте.

1.5 Нормативная база для выполнения работ

Все работы должны оказываться в соответствии с требованиями следующих документов:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01.11.2013 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСБ России от 10.07.2014 № 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 криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

1.6 Границы проведения работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации и оказания услуги по авторскому надзору за созданием системы защиты персональных данных

Границы проведения работ и оказания услуги включают -
следующие объекты размещения информационных систем персональных данных:

- G-Drive Arena – г. Омск, ул. Лукашевича, д. 35;
- Хоккейная Академия Авангард, Ассоциация «ХК «Авангард» – г. Омск, пр. Мира, д. 1Б;
- Клиентский Центр Авангард, ООО «ХК «Авангард» - г. Омск, ул. Ленина д. 20;
- Дата-Центр ПАО «Ростелеком» – г. Москва, ул. Коровинское шоссе 41;
- Дата-Центр АО «СофтЛайн Трейд» –г. Москва, Алтуфьевское ш., д. 33Г.

ИСПДн:

- до 13 ИС (Приложение №2 к Техническому заданию).

2 Требования к составу и содержанию работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации

Услуга включает в себя следующие этапы:

- Этап 1. Формирование требований к защите информации, содержащейся в информационных системах, где осуществляется обработка персональных данных;
- Этап 2. Разработка технического задания на создание системы защиты персональных данных;
- Этап 3. Разработка организационно-распорядительной документации и анализ защищенности информационных систем, где осуществляется обработка персональных данных;
- Этап 4. Оценка соответствия реализованных мер защиты персональных данных для информационных систем, где осуществляется обработка персональных данных.

2.1 Этап 1. Формирование требований к защите информации, содержащейся в информационных системах, где осуществляется обработка персональных данных

В рамках данного этапа Подрядчик должен:

- осуществить подготовку к проведению обследования;
- осуществить сбор и анализ исходных данных об обрабатываемых ПДн, ИСПДн и о применяемых мерах защиты информации;
- разработать модель угроз безопасности ПДн при их обработке в ИСПДн;
- определить необходимые уровни защищенности ПДн при их обработке в ИСПДн;
- провести оценку соответствия текущего состояния защищенности ПДн требованиям законодательства;
- разработать Протокол информационного обследования;
- определить требования к СЗПДн.

2.1.1 Подготовка к проведению обследования

Сразу после заключения договора на проведение работ и подписания соглашения о конфиденциальности должна быть проведена инициирующая встреча, на которой специалисты Подрядчика, совместно с Заказчиком определяют:

- круг лиц для проведения интервьюирования и анкетирования;
- состав проектной команды от Заказчика и Подрядчика;
- общий план проведения обследования.

Также на инициирующей встрече Подрядчик должен передать Заказчику опросные формы для сбора исходных данных. В дальнейшем Подрядчик должен оказывать консультационную помощь по заполнению переданных Заказчику опросных форм.
После получения заполненных опросных форм Подрядчик должен приготовить документ «График проведения интервью», представляющий собой таблицу с указанием ФИО и подразделения планируемых к проведению интервью специалистов Заказчика, даты, времени, длительности и тематики каждого интервью.

В дальнейшем сбор необходимой информации должен быть осуществлен несколькими основными способами:

- изучением документации, представленной Заказчиком:
  - по организационной структуре;
  - по процессам деятельности;
  - по технической инфраструктуре (оборудование, программное обеспечение, каналы связи и т. п.);
  - по существующим техническим средствам и организационным мерам обеспечения безопасности ПДн;
  - результаты предыдущих обследований и аудитов (если таковые имели место быть);
- проведением интервью с ключевыми работниками Заказчика. Круг интервьюируемых лиц может включать:
  - руководителей отделов, осуществляющих автоматизированную, неавтоматизированную и смешанную обработку персональных данных (например, бухгалтерия, отдел кадров, отдел компенсаций и льгот, юридический и финансовый департаменты, канцелярию и т. п.);
  - специалистов технических управлений, ответственных за функционирование ИСПДн;
  - специалистов по информационной, экономической и физической безопасности;
- анкетированием отдельных сотрудников службы безопасности, руководства, пользователей ИСПДн и технических подразделений Заказчика, задействованных в обработке информации, содержащей ПДн;
- обследованием процессов и средств обработки ПДн, включая сетевую инфраструктуру, средства защиты информации и автоматизированные рабочие места (далее – АРМ).

2.1.2 Сбор и анализ исходных данных об обрабатываемых ПДн, ИСПДн и о применяемых мерах защиты информации

На данном этапе должен быть осуществлен сбор и детальный анализ информации об информационных системах Заказчика (Приложение №2 к Техническому заданию), обрабатывающих ПДн, о применяемых Заказчиком организационных и технических мерах защиты информации, а также выполнен анализ информационных потоков (внутри и вне компании Заказчика), в рамках которых осуществляется передача ПДн. Специалистами Подрядчика должны быть выполнены следующие работы:

- определение состава и содержания ПДн, обрабатываемых в ИСПДн Заказчика и подлежащих защите (может отличаться от состава указанных в Приложении №1 к Техническому заданию);
- документальная фиксация перечня обрабатываемых ПДн, цели и основания обработки ПДн, а также сроки их хранения;
- исследование процедур обработки ПДн с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, защищенности процедуры передачи данных.
- анализ сетевой архитектуры;
- анализ способов ввода ПДн в ИСПДн, их жизненный цикл, обработка, передача, архивное хранение и уничтожение (анализ информационных потоков);

- определение всех приложений, которые собирают, хранят или обрабатывают ПДн;
- анализ действующих программ долгосрочного хранения ПДн;
- выявление и анализ всех помещений, где хранятся ПДн, включая вычислительные центры, серверные комнаты, офисные помещения и т.п.;
- анализ существующих версий программного и аппаратного обеспечения, которые входят в состав ИСПДн;
- анализ потоков ПДн между приложениями, информационными системами и компонентами инфраструктуры;
- анализ имеющейся организационно-распорядительной и нормативной документации по информационной безопасности и защите ПДн;
- анализ применяемых организационных мер защиты информации;
- анализ применяемых средств защиты информации.

Также в рамках сбора данных Подрядчиком должна быть выполнена проверка неавтоматизированной и смешанной обработки ПДн на их соответствие требованиям 152-ФЗ. При этом должно проверяться:

- порядок информирования лиц, осуществляющих обработку ПДн без использования средств автоматизации, о факте обработки ими ПДн;
- состав и содержание типовых форм документов;
- порядок ведения журналов (реестров, книг), содержащих ПДн, необходимых для однократного пропуска субъекта ПДн на территорию, на которой находится оператор;
- меры по обеспечению раздельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн;
- порядок уничтожение или обезличивание ПДн на материальном носителе (в том числе части ПДн, если это допускается материальным носителем);
- порядок хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях;
- условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним.

Кроме того, должны быть определены места хранения ПДн (материальных носителей) и установлен перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Все результаты сбора и анализа данных должны быть отражены в соответствующем разделе «Протокола информационного обследования».

2.1.3 Разработка модели угроз безопасности ПДн при их обработке в ИСПДн

Угрозы безопасности ПДн должны быть определены по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей ИСПДн, возможных способов реализации угроз безопасности ПДн и последствий от нарушения свойств безопасности ПДн (конфиденциальности, целостности, доступности).

При определении угроз безопасности ПДн должны быть учтены:

- структурно-функциональные характеристики ИСПДн, включающие структуру и состав ИСПДн;

- физические, логические, функциональные и технологические взаимосвязи между сегментами ИСПДн, с иными информационными системами и информационно-телекоммуникационными сетями;
- режимы обработки информации в ИСПДн и в ее отдельных сегментах;
- также иные характеристики ИСПДн, применяемые информационные технологии и особенности ее функционирования.

Модель угроз безопасности персональных данных, обрабатываемых в ИСПДн Заказчика, должна быть разработана отдельным документом и содержать описание ИСПДн и их структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИСПДн, способов реализации угроз безопасности ПДн и последствий от нарушения свойств безопасности информации.

Должна быть разработана общая Модель угроз безопасности ПДн для всех ИСПДн (Приложение №2 к Техническому заданию).

При разработке моделей угроз должны быть учтены результаты ранее проводимых моделирований угроз безопасности ПДн (при наличии таких результатов у Заказчика).

Также, по результатам моделирования угроз в Протоколе информационного обследования должны быть приведены рекомендации по выбору мер защиты информации для нейтрализации выявленных актуальных угроз безопасности ПДн.

2.1.4 Определение необходимых уровней защищенности ПДн при их обработке в ИСПДн

На данном этапе Подрядчиком должны быть проведены определение объема, типа и категорий, обрабатываемых в ИСПДн персональных данных, а также определен уровень защищенности ПДн в соответствии с требованиями, установленными в Постановлении Правительства №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

По результатам выполнения работ должен быть разработан проект документа «Акт определения необходимого уровня защищенности ПДн при их обработке в ИСПДн Заказчика» (для каждой ИСПДн должен быть разработан отдельный акт).

В случае, если у Заказчика уже имеются акты определения уровней защищенности ПДн – Подрядчик должен выполнить их актуализацию.

2.1.5 Оценка соответствия текущего состояния защищенности ПДн требованиям законодательства

На данном этапе должна быть проведена оценка степени выполнения требований законодательства по обеспечению безопасности ПДн. Оценка соответствия должна проводиться на основании следующих документов:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 №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 криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

При составлении данной оценки используются результаты анализа угроз безопасности ПДн в ИСПДн, а также результаты определения уровня защищенности ПДн при их обработке в ИСПДн. Результаты оценки соответствия должны быть отражены в соответствующем разделе «Протокола информационного обследования».

2.1.6 Разработка Протокола информационного обследования

По завершении всех указанных выше работ Подрядчик должен получить полное представление об инфраструктуре ИСПДн, о применяемых мерах защиты ПДн и о процессах обработки ПДн в компании Заказчика. Должны будут описаны технология обработки ПДн, полный перечень серверов, приложений и компонентов сетевой инфраструктуры, обслуживающих ИСПДн, и полный перечень всех лиц, ответственных за соблюдение требований по защите ПДн.

По результатам обследования существующей системы защиты Заказчика в Протокол информационного обследования должны будут включены рекомендации о возможности использования текущих решений в проекте по построению системы защиты ПДн.

Результатом анализа документов и обследования процессов обработки и защиты ПДн должны стать рекомендации о совершенствовании процессов обработки и защиты ПДн, оформленные в качестве соответствующего раздела Протокола информационного обследования.

2.1.7 Определение требований к СЗПДн

Требования к СЗПДн должны быть определены в зависимости от уровней защищенности ПДн и актуальных угроз безопасности информации, включенных в модели угроз безопасности ПДн.

Для определения всех необходимых для защиты ИСПДн Заказчика требований Подрядчиком должно быть подготовлено Техническое задание на создание СЗПДн. Техническое задание должно быть разработано с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и, в том числе, должно содержать:

- цель и задачи СЗПДн;
- перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать СЗПДн;
- общий перечень объектов защиты;
- требования к мерам и средствам защиты информации, применяемым в СЗПДн;
- требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

2.2 Этап 2. Разработка технического задания на создание системы защиты персональных данных

Техническое задание на создание СЗПДн должно быть разработано с учетом определенных уровней защищенности ПДн, модели угроз безопасности ПДн и методических документов ФСТЭК России и ФСБ России.

Структура и содержание технического задания на создание СЗПДн должны разрабатываться в соответствии с требованиями документа ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы» и должны учитывать требования к установленным уровням защищенности ПДн в ИСПДн.

В состав создаваемой СЗПДн должны входить следующие подсистемы:

- подсистема антивирусной защиты;
- подсистема межсетевого экранирования и обнаружения вторжений;
- подсистема защиты от атак типа DDoS;
- подсистема защиты среды виртуализации;
- подсистема защиты от несанкционированного доступа;
- подсистема защиты web-приложений;
- подсистема криптографической защиты информации;
- подсистема сбора и анализа событий безопасности;
- подсистема анализа защищенности.

Должна быть проведена оценка достаточности существующих подсистем в части требуемой производительности, количества лицензий и т.п.

При разработке ТЗ на СЗПДн должна быть учтена модель угроз в части скорректированных мер защиты.

В состав подсистемы антивирусной защиты должны входить:

- модуль централизованного управления компонентом;
- модуль локального управления компонентом;
- модуль антивирусной защиты среды виртуализации;
- модуль антивирусной защиты АРМ;
- модуль администрирования.

В состав подсистемы межсетевого экранирования и обнаружения вторжений должны входить:

- компонент защиты периметра;
- компонент централизованного управления;
- компонент централизованного сбора событий.

В состав подсистемы защиты от атак типа DDoS:

- компонент защиты от атак типа DDoS.

В состав компонент защиты среды виртуализации должны входить:

- основной сервер авторизации;
- резервный сервер авторизации;
- агент аутентификации;
- компонент защиты гипервизоров;
- компонент защиты средства управления средой виртуализации.

В состав подсистемы защиты от несанкционированного доступа должны входить:

- сервер централизованного управления;
- модуль защиты АРМ.

В состав подсистемы защиты web-приложений должны входить:

- компонент защиты web-приложений, опубликованных в сети Интернет;
- компонент защиты внутренних web-приложений.

В состав подсистемы криптографической защиты должны входить:

- модуль управления криптографической сетью;
- модуль криптографической защиты каналов связи;
- модуль криптографической защиты АРМ пользователей.

В состав подсистемы сбора и анализа событий безопасности должны входить:

- компонент централизованного управления подсистемой;
- компонент анализа событий безопасности;
- компонент сбора событий безопасности;
- компонент хранения событий.

В состав подсистемы анализа защищенности должны входить:

- компонент консолидации;
- компонент управления;
- сканер безопасности.

Перечень подсистем и модулей СЗПДн может быть скорректирован по результатам обследования ИСПДн Заказчика.

Согласно требованиями ФСТЭК России и ФСБ России, применяемые в составе СЗПДн СЗИ и СКЗИ должны иметь соответствующие сертификаты для использования в ИСПДн.

Результатом работ на данном этапе должно быть техническое задание на создание СЗПДн.

2.3 Этап 3. Разработка организационно-распорядительной документации и анализ защищенности информационных систем, где осуществляется обработка персональных данных

2.3.1 Актуализация комплекта проектов организационно-распорядительных документов по вопросам защиты информации в ИС

Организационно-распорядительная документация должна быть разработана (или доработана на основе существующих документов) в соответствии с требованиями технического задания на СЗПДн и направлена, в том числе, на приведение процессов обработки и защиты ПДн в соответствие требованиям законодательства РФ в области обработки и защиты ПДн.

Состав организационно-распорядительная документации:

1. Политика обработки и обеспечения безопасности персональных данных.
2. Положение об обработке и защите персональных данных, включая:
   - форму акта определения уровня защищенности персональных данных, обрабатываемых в ИСПДн;
   - форму акта оценки возможного вреда субъектам персональных данных при реализации угроз безопасности персональных данных;

- форму согласия субъекта на обработку персональных данных (общая);
- форму дополнительного соглашения (поручения на обработку персональных данных) к договору;
- лист ознакомления с организационно-распорядительными документами по вопросам обработки и обеспечения безопасности персональных данных.

3. Положение о порядке обработки персональных данных без использования средств автоматизации.
4. Положение об ответственном за организацию обработки персональных данных.
5. Положение об ответственном за обеспечение безопасности персональных данных.
6. Регламент контроля обеспечения безопасности персональных данных, включая:
   - план внутренних проверок;
   - журнал контроля обеспечения безопасности персональных данных;
   - отчет по контролю соответствия защитных мер персональных данных.
7. Порядок рассмотрения запросов субъектов персональных данных и контролирующих органов, включая формы:
   - журнала регистрации обращений и запросов субъектов персональных данных;
   - обращения субъекта персональных данных на предоставление персональных данных;
   - предоставления сведений, запрашиваемых субъектом персональных данных;
   - уведомления субъекта персональных данных об изменении персональных данных;
   - отзыва согласия субъекта на обработку персональных данных;
   - уведомления субъекта персональных данных об уничтожении персональных данных.
8. Инструкция персоналу по безопасности персональных данных.
9. Инструкция по организации обращения с защищаемыми носителями персональных данных, включая формы:
   - журнала учета материальных носителей персональных данных;
   - журнала приема-выдачи съемных носителей персональных данных;
   - журнала учета материальных носителей биометрических персональных данных;
   - акта об уничтожении персональных данных.
10. Инструкция по организации регистрации событий безопасности.
11. Инструкция по организации резервного копирования и восстановления данных, включая формы:
    - перечня информации для резервного копирования;
    - заявки на восстановление.
12. Инструкция по организации парольной защиты.
13. Инструкция по организации антивирусной защиты.
14. Паспорт ИСПДн.
15. Перечень обрабатываемых персональных данных.
16. Перечень лиц и подразделений, допущенных к обработке персональных данных.
17. Перечень информационных систем, где обрабатываются персональные данные.
18. Акт определения уровня защищенности персональных данных.
19. Акт оценки возможного вреда субъектам персональных данных.
20. Приказ об утверждении экспертной комиссии.
21. Приказ о назначении ответственных лиц.
22. Приказ об утверждении журнала регистрации посетителей, включая форму журнала учета посетителей.

23. Приказ об утверждения перечня материальных носителей персональных данных, включая перечень материальных носителей персональных данных.
24. Приказ об утверждении форм согласий.
25. Уведомление об обработке (о намерении осуществлять обработку) персональных данных.
26. Инструкция по размещению согласия на сайте.
27. Инструкция по размещению баннера на обработку cookie-данных.
28. Приказ об организации защиты персональных данных, с использованием средств криптографической защиты информации в информационной системе персональных данных.
29. Порядок организации функционирования криптосредств.
30. Инструкция ответственному за эксплуатацию средств криптографической защиты информации.
31. Инструкция пользователю средств криптографической защиты информации.

Перечень разрабатываемых документов может быть пересмотрен по результатам выполнения предыдущих этапов работ и по согласованию с Заказчиком.

2.3.2 Анализ защищенности ИС

В рамках анализа защищенности Подрядчик, с применением специальных технических средств, должен провести сканирование компонентов ИСПДн Заказчика на наличие уязвимостей. Результаты сканирования должны быть обобщены в Отчете об анализе уязвимостей.

Перед проведением испытаний по оценке соответствия Заказчик должен устранить все выявленные уязвимости, а Подрядчик должен подтвердить устранение уязвимостей путем проведения повторного сканирования.

В случае невозможности устранения какой-либо уязвимости Заказчик должен реализовать компенсирующие меры, направленные на невозможность реализации уязвимости. Подрядчик, в свою очередь, должен оказать консультационную поддержку в выборе и реализации компенсирующих мер.

2.4 Этап 4. Оценка соответствия реализованных мер защиты персональных данных для информационных систем, где осуществляется обработка персональных данных

Оценка соответствия реализованных мер защиты ПДн должна быть выполнена на основании программы и методики оценки соответствия реализованных мер защиты ПДн, разрабатываемой Подрядчиком и согласованной Заказчиком до начала проведения оценки.

Проведение оценки соответствия реализованных мер защиты ПДн должно включать в себя:

- разработку программы и методик проведения оценки соответствия реализованных мер защиты ПДн;
- оценку соответствия реализованных мер защиты ПДн разработанной программе и методикам;
- разработку Заключения о соответствии реализованных мер защиты ПДн.

Программа и методики проведения оценки соответствия должна содержать перечень конкретных работ, которые требуется провести для оценки и подтверждения

выполнения предъявляемых требований по защите ПДн и перечень объектов, подлежащих оценке.

Программа и методики проведения оценки соответствия могут быть уточнены и скорректированы по согласованию с Заказчиком в ходе самой оценки.

В ходе оценки соответствия реализованных мер защиты ПДн должны быть выполнены:

- анализ структуры ИСПДн, информационных потоков, комплекса технических средств и программного обеспечения, разработанной документации на СЗПДн;
- оценка правильности установления необходимых уровней защищенности ПДн, обрабатываемых в ИСПДн Заказчика;
- оценка правильности выбора и применения продукции, используемой для защиты ПДн;
- оценка корректности нормативного обеспечения;
- оценка достаточности и адекватности мер защиты для блокирования (нейтрализации) угроз безопасности ПДн;
- проведение испытаний в реальных условиях эксплуатации ИСПДн.

По результатам проведения оценки соответствия Подрядчиком оформляется заключение, содержащее оценку соответствия ИСПДн требованиям по защите ПДн, вывод об соответствия реализованных мер защиты ПДн, рекомендации по контролю за функционированием ИСПДн, рекомендации по устранению недостатков (при их наличии).

3 Требования к составу и содержанию подготовительных мероприятий

Перед оказанием услуг Подрядчик должен:

- обеспечить привлечение к оказанию услуг специалистов в количестве, необходимом для оказания Услуг в установленные сроки;
- представить ООО «ХК Авангард» список работников, которые будут проводить выездные работы на объектах ООО «ХК Авангард» с осуществлением доступа к объектам защиты - серверные комнаты, рабочие станции и т.п. (при необходимости).

При подготовке к оказанию услуг ООО «ХК Авангард» назначает ответственное лицо, наделённое соответствующими полномочиями для обеспечения оказания услуг Подрядчиком на территории ООО «ХК Авангард», а также для организации взаимодействия с должностными лицами ООО «ХК Авангард» и для обеспечения дистанционного сбора информации (анкетирование, переписка и т.п.).

При оказании услуг Заказчик должен:

- обеспечить доступность работников Заказчика, с которыми необходимо провести интервьюирование (перечень лиц, подлежащих интервьюированию, определяется Заказчиком на основе перечня необходимой для оказания услуг информации, запрашиваемой Подрядчиком), а также лиц, экспертное мнение которых необходимо выяснять при оказании услуг;
- предоставить работникам Исполнителя контролируемый доступ в помещения, в которых ведётся обработка информации, а также к техническим средствам обработки информации – серверам, сетевому оборудованию, рабочим станциям, принтерам и т.п. (при необходимости);
- предоставить Исполнителю всех необходимых сведений по его запросу.

Подрядчик обязуется соблюдать правила внутреннего трудового распорядка, охраны труда, техники безопасности и противопожарной охраны на территории Заказчика, а также эксплуатационной документации к техническим средствам.

4 Требования к документированию

В результате выполнения работ Подрядчиком должны быть разработаны следующие документы:

- График проведения интервью;
- Протокол информационного обследования;
- Модель угроз безопасности ПДн при их обработке в ИСПДн (общая модель угроз безопасности для всех ИСПДн);
- Форма Акта определения необходимого уровня защищенности ПДн при их обработке в ИСПДн Заказчика (для каждой ИСПДн готовится отдельный Акт);
- Техническое задание на создание СЗПДн;
- Проекты организационно-распорядительной документации;
- Отчет об анализе уязвимостей;
- Программа и методики проведения оценки соответствия реализованных мер защиты ПДн;
- Заключение об соответствии реализованных мер защиты ПДн.

Язык оформления документации – русский, за исключением общепринятых названий и оригинальных наименований программно-аппаратных средств импортного производства.

Вся документация должна быть оформлена на электронном и бумажных носителях в одном экземпляре. Состав документации может быть дополнен в ходе оказания услуг.

5 Требования к составу услуги по авторскому надзору за созданием системы защиты персональных данных

Этапность и состав услуги по авторскому надзору за созданием системы защиты персональных данных:

- Этап 1. Анализ защищенности информационных систем, где осуществляется обработка персональных данных (повторные мероприятия);
- Этап 2. Оценка соответствия реализованных мер защиты персональных данных для информационных систем, где осуществляется обработка персональных данных (повторные мероприятия).

Оценка соответствия реализованных мер защиты персональных данных должна быть выполнена в соответствии с программой и методиками оценки соответствия реализованных мер защиты персональных данных, разработанной Подрядчиком и согласованной Заказчиком на моменте выполнения работ по приведению процессов обработки и защиты персональных данных в соответствие требованиям законодательства Российской Федерации.

Программа и методики проведения оценки соответствия могут быть уточнены и скорректированы по согласованию с Заказчиком в ходе самой оценки.

По результатам проведения повторных мероприятий Подрядчиком оформляется заключение, содержащее оценку соответствия информационных систем, где осуществляется обработка персональных данных (Приложение №2 к Техническому заданию), требованиям по защите персональных данных.