ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Обследование процессов обработки персональных данных
на соответствие требованиям законодательства Российской Федерации.

Кемерово
2025

ОГЛАВЛЕНИЕ

1. ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

АО	– акционерное общество
ИС	– информационная система
ИСПДн	– информационная система персональных данных
ИТКС	– информационная телекоммуникационная сеть
ООО	– общество с ограниченной ответственностью
ОРД	– организационно-распорядительная документация
ПДн	– персональные данные
ФЗ	– Федеральный закон
ФСБ России	– Федеральная служба безопасности
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю

2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее техническое задание является исходным техническим документом для предъявления требований к обследованию обработки персональных данных в организациях, на соответствие требованиям законодательства Российской Федерации:

- Обследование информационной инфраструктуры,
- Оценка соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности персональных данных;
- Определение уровня защищенности ИСПДи;
- Актуализация и (или) разработка организационно-распорядительной документации;
- Разработка дорожной карты по приведению в соответствие или выводы о соответствии;

Плановые сроки реализации работ в соответствии с требованиями технического задания: в течение 120 рабочих дней с момента заключения договора

3. ПЕРЕЧЕНЬ ДОКУМЕНТОВ, НА ОСНОВАНИИ КОТОРЫХ ВЫПОЛНЯЮТСЯ РАБОТЫ

В процессе выполнения услуг, предусмотренных настоящим техническим заданием, должны использоваться следующие нормативные документы:

- Федеральный закон от 26 июля 2006 г. № 152-ФЗ «О персональных данных»;
- «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687;
- «Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденный постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119;
- «Состав и содержание 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»., утвержденные приказом ФСБ России от 10 июля 2014 г. № 378;

- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21;
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»;
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 мая 2017 г. № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»;
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 октября 2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»;
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».

4. НАЗНАЧЕНИЕ И ЦЕЛИ ПРОВЕДЕНИЯ РАБОТ

Основной целью проекта является повышение уровня безопасности информации, циркулирующей в информационной телекоммуникационной инфраструктуре компаний холдинга и соответствие требованиям законодательства Российской Федерации по обработке персональных данных.

5. ОБЩИЕ СВЕДЕНИЯ

Область оказания услуг включает в себя процессы (бизнес-процессы) информационные системы и ИТ-инфраструктуру, эксплуатируемую Заказчиком.

№	Название площадки и расположение (наименование, адрес) Наименование ИСПДн	Количество рабочих станций		Количество серверов	
		Всего	Связанных с обработкой ПДн	Всего	Связанных с обработкой ПДн
АО «КТК», Кемерово, ул. 50 лет Октября,4					
1	1С: УПП	292	23	1	1
2	1С: ЗУП	10	10	1	1
3	СКУД	0	0	1	1
4	AD	6	6	2	2
5	Почта (Адресная книга)	800	800	2	2
6	OTRS (Регистрация инцидентов)	30	30	1	1
Филиал АО «КТК» разрез «Виноградовский»					
1	1С: ERP ГДП	133	29	1	1
2	СКУД	2	2	1	1
3	AD	6	6	2	2
ООО «ТЭК Мереть», Кемеровский район, с. Старопестерево					
1	1С: УПП	99	19	1	1
2	1С: ЗУП	23	23	1	1
3	СКУД	0	0	1	1
ООО «Кузбасстопливосбыт»					
1	1С: УПП	138	28	0	0
2	1С: ЗУП	33	33	0	0
3	1С: УТСК	76	76	1	1
ООО «КТК Консалтинг», Кемерово, ул. 50 лет Октября,4					
1	1С: УПП	125	25	0	0
2	1С: ЗУП	9	9	0	0
ООО «Каскад Гео», Кемерово, ул. 50 лет Октября,4					
1	1С: УПП	125	25	0	0
2	1С: ЗУП	10	10	0	0
ООО «Кузбасская энергокомпания», Кемерово, ул. 50 лет Октября,4					
1	1С: УПП	18	3	0	0
2	1С: ЗУП	7	7	0	0
ООО «НТК», г. Новосибирск, ул. Некрасова, д. 50, 7 этаж					
1	1С: УПП	97	13	1	1
2	1С: ЗУП	20	20	0	0
3	1С: УТСК	74	74	0	0
АО «Алтайская топливная компания», г. Барнаул, ул. Деповская, 7					
1	1С: УПП	71	16	0	0
2	1С: ЗУП	14	14	0	0
3	1С: УТСК	19	19	0	0
ООО «ТрансУголь», Омская обл, Крутинский р-н, Крутинка рп, Лесная ул, дом 1					
1	1С: УПП	54	10	0	0
2	1С: ЗУП	13	13	0	0
3	1С: УТСК	2	2	0	0
АО «Каскад-энерго», г. Анжеро-Судженск, ул. Ленина, д. 4					
1	1С: УПП	84	22	1	1
2	1С: ЗУП	19	19	0	0

3	Коминтех. АРМ Расчет квартплаты	5	5	1	1
ООО «Новая сетевая компания», г. Анжеро-Судженск, ул. Ленина, д. 4					
1	1С: УПП	9	9	0	0
2	1С: ЗУП	9	9	0	0
ООО «Управляющая компания Анжерская», Анжеро-Судженск г, Камышинская ул, дом № 15					
1	1С: Бухгалтерия	2	2	0	0
2	1С: ЗУП	3	3	1	1
3	Коминтех. АРМ Расчет зарплаты	8	2	1	1

В случае выявления, в рамках обследования, иных информационных системы данные информационные системы также должны быть обследованы

6. ТРЕБОВАНИЯ К РАБОТАМ

6.1. Обследование информационной инфраструктуры, оценка эффективности Комплексной системы управления информационной безопасности и оценка соответствия требованиям законодательства Российской Федерации в области обеспечению безопасности информации

Задачи работ:

- Провести очное обследование обработки персональных данных в организациях, на соответствие требованиям № 152-ФЗ «О персональных данных». Выездное обследование осуществляется по адресу центрального офиса: г. Кемерово, ул. 50 лет Октября, д. 4. Обследование филиалов проводится удалённо путём подключения из центрального офиса и/или проведение интервью с помощью ВКС;
- На данном этапе требуется собрать сведения об обработки персональных данных в организациях;
- Определение наличия на предприятии, на котором расположены объекты информатизации, наличия службы безопасности, службы администраторов (автоматизированных систем, сетей, баз данных);
- Сбор информации о подразделениях, участвующих в организации и осуществлении работ по защите информации, о лицах, ответственных за безопасность информации;
- Определение полного и точного наименования исследуемых объектов информатизации и их назначение;
- Анализ процессов, в рамках которых осуществляется обработка персональных данных;

- Определение целей и оснований обработки информации, состава обрабатываемой информации, категорий субъектов информации, необходимого срока обработки информации, перечня действий с информаций, мест и форм хранения информации;
- Определение особенностей расположения объектов информатизации с указанием границ контролируемой зоны;
- Анализ информации о физической охране технических средств на объектах информатизации;
- Определение наличия объектов и характера взаимодействия этих объектов информатизации друг с другом и с иными/сторонними объектами информатизации;
- Формирование перечня ИСПДн;
- Анализ имеющейся проектной и эксплуатационной документации на объекты информатизации и другие исходные данные по объектам информатизации, влияющие на безопасность информации;
- Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации;
- Определение применяемых средств защиты информации и наличии у них сертификатов ФСТЭК России и/или ФСБ России (при необходимости);
- Оценка соответствия выполнения требований законодательства Российской федерации в области обеспечения безопасности информации.

Отчетность:

Результаты работ должны быть отражены в Отчете по результатам обследования и оценке соответствия требованиям законодательства Российской Федерации в области обеспечению безопасности информации.

6.2. Анализ организации хранения персональных данных с применением технического решения DCAP (Data-Centric Audit and Protection)

С целью оценки безопасности персональных данных в ходе работ должна быть предоставлена лицензия на систему контроля и управления доступом к неструктурированным данным (DCAP-решение) сроком на 1-2 месяца для обеспечения поиска и классификации персональных данных на серверах хранения.

Основные требования к функциональным возможностям DCAP-решения:

- Сканирование и анализ файловых серверов (Windows, Linux) и систем хранения данных (СХД) с выявлением персональных данных;

- Классификация данных по категориям с использованием поиска по словам, фразам, регулярным выражениям и нейросетевым методам;
- Автоматическое обнаружение чувствительной информации (паспортные данные, СНИЛС, банковские карты и др.);
- Анализ структуры прав доступа к данным и выявление рисков безопасности;
- Аудит доступа пользователей к файловым ресурсам;
- Формирование отчётности о размещении и защищённости персональных данных.

6.3. Разработка актов определения уровня защищённости

На основании собранных данных должно быть проведено определение уровня защищенности ИСПД в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119.

Отчетность:

Результаты работ должны быть отражены в:

- Актах определения уровня защищенности;

6.4. Актуализация и (или) разработка организационно-распорядительной документации.

Задачи работ:

- Провести корректировку имеющихся ОРД;
- В случае отсутствия необходимых ОРД, осуществить их разработку.

Перечень документов подлежащих разработке:

1. **Приказы:**
   1. **О создании комиссии по защите персональных данных;**
   2. **Об утверждении правил оценки вреда, который может быть причинён субъектам персональных данных;**
      - *2.1. Приложение – Правила оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных;*
      - *2.2. Приложение - форму акта оценки потенциального вреда субъектам персональных данных.*
   3. **О назначении ответственных;**
      - *3.1. Приложение – Инструкция ответственного за организацию обработки персональных данных;*

3.2. Приложение – Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных;

3.3. Приложение – Инструкция администратора безопасности информационных систем персональных данных.

4. **Об утверждении перечня информационных систем персональных данных и допущенных должностей работников**
   - *4.1. приложение – Перечень информационных систем персональных данных*
   - *4.2. приложение– Перечень должностей работников, допущенных к обработке персональных данных*
5. **Об организации режима обеспечения безопасности помещений, в которых ведется обработка персональных данных**
   - *5.1. приложение – Перечень помещений, в которых ведется обработка персональных данных*
   - *5.2. приложение– Правила доступа работников в помещения, в которых ведется обработка персональных данных*
6. **Об утверждении инструкций по защите персональных данных**
   - *6.1. приложение – Инструкция пользователя информационных систем персональных данных*
   - *6.2. приложение – Инструкция по парольной защите информации*
   - *6.3. приложение – Инструкция по антивирусной защите*
   - *6.4. приложение – Инструкция по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных*
   - *6.5. приложение – Порядок обращения со съемными машинными носителями персональных данных*
7. **Об обращении со средствами криптографической защиты информации**
   - *7.1. Приложение – Инструкция по обращению со средствами криптографической защиты информации*
   - *7.2. Приложение – Перечень режимных помещений, выделенных для установки средств криптографической защиты информации и хранения ключевых документов к ним*
   - *7.3. приложение – Перечень защищенных хранилищ, предназначенных для хранения средств криптографической защиты информации, ключевых документов, эксплуатационной и технической документации к средствам криптографической защиты информации*
   - *7.4. приложение – Перечень работников, допущенных к работе с шифровальными (криптографическими) средствами защиты информации*
8. **Об утверждении регламента реагирования на инциденты информационной безопасности в информационных системах персональных данных**

8.1. Приложение – регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных.

9. О разрешительной системе доступа

9.1. Приложение – Положение о разрешительной системе доступа в информационных системах персональных данных.

10. Об утверждении положения об организации обработки персональных данных без использования средств автоматизации

10.1. Приложение – Положение об организации обработки персональных данных без использования средств автоматизации.

11. О закреплении мест хранения ПДн

12. Об утверждении регламента проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

12.1. приложение – Регламент проведения внутреннего контроля соответствия обработки персональных данных в организации требованиям к защите персональных данных

12.1.1. Плана проведения внутреннего контроля соответствия обработки персональных данных

13. Об утверждении Положения об обработке и обеспечении безопасности персональных данных

13.1. Приложение – Положение об обработке и обеспечении безопасности персональных данных.

14. Об утверждении Политики в отношении обработки персональных данных

14.1. Приложение – Политика в отношении обработки персональных данных

15. О закреплении местонахождения баз данных

16. Об утверждении порядка проведения регулярного мониторинга законодательства о ПДн

16.1. Приложение – Порядок проведения регулярного мониторинга законодательства о ПДн.

17. О проведении сканирования уязвимостей

2. Акты:

1. Определения уровня защищенности персональных данных при их обработке в информационной системе (для каждой ИС);
2. Оценки вреда, который может быть причинен субъектам персональных данных.

3. Заключения:

1. О подготовке и допуске к самостоятельной работе со средствами криптографической защиты;
2. О возможности эксплуатации средств криптографической защиты информации на автоматизированных рабочих местах.

4. Формы:

1. Согласие на обработку персональных данных;
2. Обязательство о неразглашении информации ограниченного доступа;

3. Договор поручения на обработку персональных данных;
4. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения;
5. Журнал учета съемных машинных носителей персональных данных;
6. Журнал поэкземплярного учета шифровальных (криптографических) средств защиты информации;
7. Журнал учета ключей от режимных помещений, карт для доступа в режимные помещения, ключей хранилищ, личных печатей от хранилищ;
8. Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки информации;
9. Журнал учета мест хранения носителей персональных данных;
10. Журнал учета лиц, осуществляющих неавтоматизированную обработку персональных данных;
11. Журнал регистрации обращений субъектов персональных данных, чьи персональные данные обрабатываются;
12. Технический (аппаратного) журнала учета средств криптографической защиты информации;
13. Акта уничтожения персональных данных;
14. Отзыв согласия на обработку персональных данных;
15. Уведомление о невозможности удаления персональных данных;
16. Акт уничтожения шифровальных (криптографических) средств;
17. Акт о проведении контроля соответствия обработки персональных данных;
18. Лицевой счет пользователя СКЗИ.

5. Дополнительные материалы:

1. Инструкция по заполнению электронной формы уведомления об обработке о намерении осуществлять обработку) персональных данных;
   Соглашение об использовании cookie-файлов.

Необходимо провести корректировку/разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты ИС в ходе ее эксплуатации.

В случае выявления потребности в разработке дополнительных ОРД, производится формирование их перечня с требованием к конкретному документу. Разработка данных документов происходит в рамках данных работ. Возможна корректировка текущего перечня ОРД с сохраняем наполнения и соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

6.5. Требования к исполнителю

Исполнитель (в том числе каждое юридическое и/или физическое лицо, выступающее на стороне одного участника) должен:

не иметь задолженности по уплате налогов (сборов, пеней, налоговых санкций) в бюджеты всех уровней и обязательных платежей в государственные внебюджетные фонды;

- не находиться в процессе ликвидации;
- не быть признанным несостоятельным (банкротом);
- на его имущество не должен быть наложен арест, экономическая деятельность участника не должна быть приостановлена;
- не находиться в реестрах недобросовестных поставщиков, указанных в подпункте 7 статьи 3 Федерального закона от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» (каждом из физических и\или юридических лиц, выступающих на стороне участника).

Исполнитель должен иметь лицензию ФСТЭК России на деятельность:

- по технической защите конфиденциальной информации в области проектирования в защищенном исполнении средств и систем информации;
- по оказанию услуг контроля защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации,
- по оказанию услуг контроля защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- по оказанию услуг по установке, монтажу, наладке, испытаний средств защиты информации.

Исполнитель должен обладать опытом работы в области защиты информации не менее 5 лет;

Исполнитель должен иметь не менее 5 штатных сотрудников с профильным образованием либо переподготовкой в области информационной безопасности;

6.6. Требование к проектному управлению

- Организация работ должна строиться таким образом, чтобы оптимизировать объем задействованных ресурсов со стороны Заказчика;
- Должен быть предложен ролевой состав проектной группы со стороны Исполнителя и Заказчика, а именно должны быть указаны лица, ответственные за управление Проектом, разработку документации, проведение технических работ;

6.7. Требования по обеспечению конфиденциальности выполнения работ

Согласно действующему законодательству и нормативным документам, принятым у Заказчика, должны приниматься следующие меры по обеспечению конфиденциальности выполнения работ:

- Информация, полученная Исполнителем в процессе выполнения работ, не может быть передана третьим лицам без согласия Заказчика;
- Исполнитель должен обеспечивать безопасность передаваемой ему информации Заказчика.

6.8. Дополнительные требования

Материалы, полученные по результатам работ, должны быть подготовлены и оформлены на русском языке с использованием MS Office 2010/2016 (Word, Excel, PowerPoint). Разрабатываемая документация должна быть представлена в электронном и при необходимости в бумажном виде в 1 экземпляре.