Утверждаю
Генеральный менеджер
ПАО «ГК «Космос»

_____ А.Ю. Швейн

«21» ноября 2017 г.

Согласовано
Член Правления, заместитель
генерального менеджера по безопасности
ПАО «ГК «Космос»

_____ А.В. Сончик

«21» 09 2017 г.

ПАО «ГК «Космос»

ОБСЛЕДОВАНИЕ ПОРЯДКА ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И РАЗРАБОТКА ТЕХНИЧЕСКОГО ПРОЕКТА НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На 9 листах

СОДЕРЖАНИЕ

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

АРМ	Автоматизированное рабочее место, рабочая станция
ИБ	Информационная безопасность
ИСПДн	Информационная система персональных данных
ОРД	Организационно распорядительная документация
ПДн	Персональные данные
РФ	Российская Федерация
СЗПДн	Система защиты персональных данных
ТЗ	Техническое задание
ФСБ	Федеральная служба безопасности Российской Федерации
ФСТЭК	Федеральная служба по техническому и экспортному контролю Российской Федерации

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Настоящее ТЗ определяет требования к работам по обследованию порядка обработки и обеспечения безопасности ПДн ПАО «ГК «Космос» и разработке технического проекта на создание СЗПДн, а также состав вышеуказанных работ.

1.2 Наименование работ: «Обследование порядка обработки и обеспечения безопасности ПДн и разработка технического проекта на создание СЗПДн».

1.3 Заказчик: ПАО «ГК «Космос». Фактический адрес: Россия, 129366, Москва, Проспект Мира, 150.

1.4 Исполнитель: определяется по результатам конкурса.

1.5 Начало работ – с момента заключения Договора между Заказчиком и Исполнителем. Окончание работ – 31 января 2017 года.

1.6 Целью выполнения работ является реализация требований законодательства РФ о порядке обработки ПДн и об обеспечении безопасности ПДн.

2. НОРМАТИВНАЯ БАЗА ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПДН

2.1 Работы должны проводиться в соответствии со следующими законами, подзаконными нормативными актами и ведомственными документами:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.;
- Приказ ФСБ России от 10 июля 2014 г. N 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»;

- ГОСТ 34.201 «Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

3. СОДЕРЖАНИЕ РАБОТ

3.1 Объем выполняемых работ предполагает:

- проведение обследования порядка обработки и защиты ПДн и разработка Отчета по результатам обследования, включающего в себя:
    - определение категорий субъектов обрабатываемых ПДн;
    - определение состава обрабатываемых ПДн;
    - определение правовых оснований для обработки ПДн;
    - установление случаев передачи ПДн третьим лицам, трансграничной передачи ПДн;
    - анализ действующих локальных нормативных актов, регламентирующих деятельность компании в области ИБ;
    - выработку рекомендаций по внесению изменений в договоры с третьими лицами и клиентами, локальные нормативно-правовые акты;
    - идентификацию ИСПДн;
    - формирование перечня ПДн в ИСПДн;
    - определение архитектуры, конфигурации и топологии ИСПДн в целом и их отдельных компонент, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами;
    - определение условий расположения ИСПДн относительно границ контролируемой зоны;
    - выработку предложений по созданию оптимальной структуры ИСПДн (при необходимости оптимизации);
    - анализ степени участия персонала в обработке ПДн;
    - определение режима обработки ПДн в ИСПДн в целом и в отдельных компонентах;
    - анализ существующих мер по защите ПДн на предмет соответствия требованиям законодательства в области ПДн;

- выявление несоответствия порядка обработки и защиты ПДн действующему законодательству РФ;
- предложение мер и мероприятий по устранению выявленных несоответствий.

- разработка Модели угроз безопасности ПДн при их обработке в ИСПДн;
- определение уровней защищенности ПДн в ИСПДн;
- разработка Технического задания на создание СЗПДн;
- разработка Технического проекта на создание СЗПДн;
- разработка проектов организационно-распорядительной документации по организации обработки и защиты ПДн.

4. РАЗРАБАТЫВАЕМЫЕ ДОКУМЕНТЫ

4.1 Ответственным за разработку отчетных документов признаётся Исполнитель. Заказчик оказывает содействие Исполнителю путем предоставления требуемых исходных данных, запрашиваемой Исполнителем существующей документации, а также путем создания условий для проведения интервью с представителями подразделений Заказчика, участвующих в обработке ПДн.

4.2 Исполнитель предоставляет следующий комплект документов:

№	Наименование отчетных документов
1.	Отчет по результатам обследования порядка обработки и защиты ПДн
2.	Модель угроз безопасности ПДн при их обработке в ИСПДн
3.	Акты определения уровней защищенности ПДн в ИСПДн
4.	Техническое задание на создание СЗПДн
5.	Технический проект на создание СЗПДн в составе:
5.1.	Пояснительная записка
5.2.	Схема структурная комплекса технических средств ИБ
5.3.	Спецификация средств защиты информации
6.	Проекты организационно-распорядительной документации в составе:
6.1.	Публичная политика обработки персональных данных
6.2.	Положение об организации обработки персональных данных
6.3.	Перечень персональных данных, обрабатываемых в Обществе
6.4.	Регламент взаимодействия с субъектами персональных данных
6.5.	Регламент предоставления доступа к персональным данным
6.6.	Перечень структурных подразделений и должностей, допущенных к обработке персональных данных
6.7.	Регламент обмена персональными данными с третьими лицами
6.8.	Регламент обработки персональных данных без использования средств автоматизации
6.9.	Перечень мест хранения бумажных носителей персональных данных
6.10	Регламент обращения с машинными носителями персональных данных
6.11.	Регламент обезличивания персональных данных
6.12.	Регламент уничтожения персональных данных
6.13.	Регламент доступа в помещения, в которых ведется обработка персональных

	данных
6.14.	Регламент взаимодействия с уполномоченными органами в сфере обработки и обеспечения безопасности персональных данных
6.15.	Регламент ответственного за организацию обработки персональных данных
6.16.	Положение об обеспечении безопасности персональных данных
6.17.	Регламент ответственного за обеспечение безопасности персональных данных
6.18.	Регламент оценки возможного вреда субъектам персональных данных
6.19.	Регламент выделения информационных систем персональных данных и определения необходимого уровня защищенности персональных данных
6.20	Перечень информационных систем персональных данных
6.21.	Регламент выбора мер по обеспечению безопасности персональных данных
6.22.	Регламент управления инцидентами информационной безопасности
6.23.	Регламент проведения периодических проверок в области обработки и обеспечения безопасности персональных данных
6.24.	Приказ о порядке обработки персональных данных
6.25.	Приказ о назначении ответственного за организацию обработки персональных данных
6.26.	Приказ о назначении ответственного за обеспечение безопасности персональных данных
6.27.	Приказ о создании комиссии по обеспечению безопасности персональных данных
6.28.	Приказ об организации режима обеспечения безопасности помещений, в которых осуществляется обработка персональных данных

5. ХАРАКТЕРИСТИКИ ОБЪЕКТОВ ПРОВЕДЕНИЯ РАБОТ

5.1 Инфраструктура ПАО «ГК «Космос» находится на площадке по адресу: Россия, 129366, Москва, Проспект Мира, 150.

5.2 Инфраструктура ПАО «ГК «Космос» включает себя около 250 АРМ; 4 ИСПДн.

6. ИСХОДНЫЕ ДАННЫЕ ДЛЯ ВЫПОЛНЕНИЯ РАБОТ

6.1 Для выполнения работ по ТЗ Исполнителю предоставляются исходные данные о Заказчике в объёме, необходимом для выполнения работ, в частности:

- описание организационно-штатной структуры;
- описание бизнес-процессов, включающих необходимость обработки ПДн;
- информацию по ИСПДн в отношении характера обрабатываемых ПДн, используемых технических средств, системного и прикладного ПО;
- сведения об IP-адресации и маршрутизации в сети;
- информацию по существующему активному сетевому оборудованию, его расположению, интерфейсам, количеству каналов связи, пропускной способности каналов связи, конфигурации;
- схемы сети на физическом и логическом уровнях;
- информацию по существующим сетям электропитания и заземления, точкам подключения оборудования, запасам по мощности в точках подключения, характеристикам заземления;

- информацию по существующим серверам и рабочим станциям, составу их аппаратного и программного обеспечения;
- внутренние ОРД в области информационных технологий, обеспечения ИБ и обработки ПДн;
- информацию о применяемых или планируемых к применению средств защиты информации;
- планы помещений, в которых установлено или должно быть установлено оборудование, используемое для обработки или защиты ПДн;
- схемы расположения оборудования в шкафах;
- положения политик обеспечения информационной безопасности Заказчика, разработанных в соответствии с ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- иные данные, необходимые для выполнения работ по ТЗ.

6.2 Форма предоставления исходных данных согласуется представителями Заказчика и Исполнителя в рабочем порядке в процессе выполнения работ.

7. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ РАБОТ И УСЛОВИЯМ ВЫПОЛНЕНИЯ РАБОТ

7.1 При производстве работ Заказчик выполняет следующие организационные мероприятия:

- осуществляет контроль за выполнением работ;
- назначает ответственных лиц за организацию работ;
- предоставляет необходимые исходные данные для выполнения работ;
- рассматривает и согласовывает (утверждает) разрабатываемые Исполнителем документы;
- обеспечивает доступ представителей Исполнителя на объекты для получения необходимой информации.

8. ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ

8.1 Исполнитель должен обладать следующими действующими лицензиями:

- лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации;
- лицензия ФСБ России на право осуществлять следующие виды деятельности: разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое

обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

8.2 Исполнитель должен иметь опыт выполнения комплексных проектов по обеспечению информационной безопасности для распределённых вычислительных сетей организаций федерального уровня.

8.3 Наличие у Исполнителя подтвержденного опыта обследования порядка обработки и защиты ПДн и создания СЗПДн.

8.4 В штате Исполнителя должно быть не менее двух специалистов, имеющих подтвержденную квалификацию (диплом о высшем образовании государственного образца) в области обеспечения информационной безопасности и обладающих опытом выполнения соответствующих проектов.

8.5 Срок деятельности Исполнителя в области оказания услуг по информационной безопасности должен быть не менее 5 лет.

Руководитель по направлению
информационной безопасности

В.П. Гаргосов