УТВЕРЖДАЮ:
Генеральный директор
ООО «АтомЭнерго»
В.Н. Маркелов

«__» _____ 2022 г.

Техническое задание на оказание услуг

Аттестация по требованиям безопасности информации, с обеспечением требуемого уровня защищенности персональных данных при их обработке в автоматизированной системе в защищенном исполнении ООО «АтомЭнерго»

Москва 2022

ПЕРЕЧЕНЬ ВИДОВ УСЛУГ на основе справочника ОКПД-2, ОКВЭД-2
для закупки которых применяется настоящее техническое задание

Код	Вид услуги
ОКПД 2: 80.10.19.000	Услуги в области обеспечения безопасности прочие
ОКВЭД 2: 63.11	Деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность

СОДЕРЖАНИЕ

РАЗДЕЛ 1. НАИМЕНОВАНИЕ УСЛУГИ

Аттестация по требованиям безопасности информации, с обеспечением требуемого уровня защищенности персональных данных при их обработке в автоматизированной системе в защищенном исполнении (далее – АСЗИ) ООО «АтомЭнерго» (далее – Заказчик).

РАЗДЕЛ 2. ОПИСАНИЕ УСЛУГИ

Подраздел 2.1 Состав (перечень) оказываемых услуг
2.1.1 В ходе оказания услуг должны быть выполнены следующие работы: – обследование объектов информатизации Заказчика, оценка соответствия АСЗИ и имеющейся системы защиты требованиям по защите информации (в части технических и организационных мер обеспечения информационной безопасности); – классификация АСЗИ как автоматизированной системы; – классификация АСЗИ как информационной системы персональных данных; – разработка модели угроз и модели нарушителя информационной безопасности и формирование частного технического задания на АСЗИ; – разработка необходимых мер (организационных и технических) по защите информации, отвечающих требованиям по защите информации, регламентированным действующим законодательством, нормативно-методическими документами ФСТЭК России и Едиными отраслевыми методическими указаниями по информационной безопасности и использованию средств защиты информации для автоматизированных систем, обрабатывающих информацию, составляющую коммерческую тайну, служебную информацию ограниченного распространения (с пометкой «Для служебного пользования»), а также персональные данные в Госкорпорации «Росатом» и ее организациях; – оказание услуг по вводу в действие средств защиты информации в соответствии с техническими решениями; – подготовка к проведению аттестационных испытаний АСЗИ и комплекта документов, необходимых для представления АСЗИ Заказчика к аттестационным испытаниям на соответствие требованиям безопасности информации в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» ФСТЭК России, а также по требованиям безопасности к определенному в процессе выполнения услуг уровню защищенности персональных данных; – проведение аттестационных испытаний АСЗИ Заказчика по требованиям безопасности информации.
Подраздел 2.2 Описание оказываемых услуг
2.2.1 Указанные в разделе 2.1 услуги необходимо оказать в семь этапов: 1. Этап 1. Обследование объектов информатизации Заказчика и классификация АСЗИ Заказчика. 2.Этап 2. Разработка модели угроз и модели нарушителя информационной безопасности. 3. Этап 3. Разработка организационно-распорядительной документации. 4. Этап 4. Разработка комплекта документации технического проекта. 5. Этап 5. Ввод в действие аппаратных и программных компонентов средств защиты на объектах Заказчика, проведение предварительных испытаний, опытной эксплуатации и приемочных испытаний. 6. Этап 6. Разработка технического паспорта.

7. Этап 7. Аттестация АСЗИ Заказчика на соответствие требованиям по защите информации в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» ФСТЭК России, а также по требованиям безопасности к определенному в процессе выполнения услуг уровню защищенности персональных данных.

2.2.2 Описание состава услуг по этапам изложено в п. 3.1.

Подраздел 2.3 Объем оказываемых услуг либо доля оказываемых услуг в общем объеме закупки

2.3.1 Услуги должны быть оказаны в полном объеме в соответствии с настоящим Техническим заданием и заключенным Договором.

РАЗДЕЛ 3. ТРЕБОВАНИЯ К УСЛУГАМ

Подраздел 3.1 Общие требования

3.1.1 Услуги по настоящему Техническому заданию оказываются по адресам:

Номер объекта	Наименование объекта	Адрес
1	Центральный офис	115432, г. Москва, проезд Проектируемый 4062-й, д. 6, стр. 25

3.1.2 Общее количество автоматизированных рабочих мест, входящих в АСЗИ – 14 шт.

3.1.3 Разрабатываемая система защиты информации АСЗИ должна удовлетворять требованиям и положениям правовых, нормативных и ведомственных отраслевых документов, приведенных в разделе 3.2 настоящего Технического задания.

3.1.4 Требования к этапам оказания услуг.

3.1.4.1 Этап 1. Обследование объектов информатизации Заказчика и классификация АСЗИ Заказчика.

В рамках выполнения услуг по Этапу 1 Исполнитель должен выполнить:

- информационное обследование информационной системы Заказчика и его основных компонентов;
- анализ существующих процессов управления ИТ-инфраструктурой, реализованных в ИС Заказчика;
- анализ существующих процессов управления и обеспечения информационной безопасности, реализованных Заказчиком;
- анализ действующих НПА в области ИБ;
- проведение анализа процедур обработки информации в информационных системах;
- классификация АСЗИ как автоматизированной системы, и как информационной системы обработки персональных данных.

В процессе выполнения услуг должна быть собрана и проанализирована информация, необходимая и достаточная для проведения следующих этапов услуг по созданию системы защиты информации, в том числе:

- состав, содержание и объем обрабатываемых в информационных системах данных;
- структура, состав и топология информационных систем;
- организация подключений информационных систем к сетям связи;
- режим обработки данных и разграничения прав доступа;

– местонахождение технических средств;

– границы контролируемой зоны и расположение объекта информатизации относительно них;

– применяемые меры и средства защиты;

– соответствие нормативной базы Заказчика требованиям руководящих документов по защите информации.

В процессе классификации информационных систем должна быть установлена необходимость классификации по следующим направлениям:

– как информационной системы персональных данных;

– как автоматизированной системы, обрабатывающей конфиденциальную информацию.

Обследование должно выполняться путем проведения анкетирования и интервьюирования уполномоченных сотрудников Заказчика, с обязательным привлечением специалистов ИТ и ИБ организации, отвечающей за обеспечение функционирования ИТ-инфраструктуры Заказчика, и путем ознакомления с действующими локальными нормативно-методическими документами.

Основными источниками получения информации о функционировании ИС и используемых механизмах защиты являются сотрудники уполномоченных подразделений Заказчика и сотрудники уполномоченных подразделений организации, отвечающей за обеспечение функционирования ИТ-инфраструктуры Заказчика, привлечение сотрудников иных смежных подразделений должно осуществляться при необходимости по согласованию с Заказчиком.

Услуги по предварительному обследованию должны оказываться Исполнителем на объектах Заказчика указанных в пункте 3.1.1.

Результатом оказания услуги по предварительному обследованию являются:

– проект акта определения уровня защищенности персональных данных;

– проект акта классификации автоматизированной системы, обрабатывающей конфиденциальную информацию;

– аналитическое обоснование необходимости создания (модернизации) СЗИ;

– проект заключения ПДТК об уровне конфиденциальности информации в АС.

3.1.4.2 Этап 2. Разработка модели угроз и модели нарушителя информационной безопасности.

На данном Этапе оказания услуг должны быть разработаны: Модель угроз и Модель нарушителя информационной безопасности.

Модель угроз должна содержать:

– структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования;

– оценку возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализ возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности);

– перечень актуальных угроз безопасности информации.

Модель нарушителя должна содержать:

– описание совокупности предположений о возможностях нарушителя, которые он в состоянии использовать для разработки и проведения атак, а также об ограничениях на эти возможности;

– определение требуемого класса средств криптографической защиты информации (далее – СКЗИ).

3.1.4.3 Этап 3. Разработка организационно-распорядительной документации.

На данном этапе должны быть разработаны следующие проекты документов:

– Положение о порядке организации и проведении работ по защите конфиденциальной информации;

– Проект приказа об определении границ контролируемой зоны;

– Перечень защищаемых ресурсов;

– Проект приказа об определении ответственных должностных лиц за выполнение требований по защите информации;

– Таблица разграничения доступа (матрица доступа);

– Описание технологического процесса обработки информации в АС;

– Инструкция по эксплуатации средств защиты информации;

– Инструкция по организации хранения и использования средств восстановления СЗИ НСД;

– Порядок изменения условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

– Инструкция по организации выдачи на печать и учету документов, содержащих конфиденциальную информацию;

– Инструкция по организации доступа в помещения;

– Инструкция администратора АС;

– Инструкция администратора безопасности информации;

– Инструкция пользователя;

– Проект журнала учета инцидентов информационной безопасности;

– Проект журнала учета машинных носителей, предназначенных для хранения информации ограниченного доступа;

– Проект журнала регистрации печати информации ограниченного доступа;

– Проект журнала учета паролей администраторов АС;

– Проект журнала периодического контроля средств защиты информации;

– Перечень правил фильтрации межсетевых экранов;

– Список пользователей, допущенных к обработке информации ограниченного доступа;

– Список пользователей, допущенных в помещения, где располагаются технические средства АС.

3.1.4.4 Этап 4. Разработка комплекта документации технического проекта.

В рамках данного этапа требуется выполнить разработку Технического проекта на создание СЗИ с указанием перечня предполагаемых к использованию сертифицированных средств защиты информации.

Результаты данного этапа должны быть отражены в следующих документах:

– Техническое задание на создание (модернизацию) СЗИ АС;

– Пояснительная записка к техническому проекту создания АС;

– Программа и методика испытаний;

– Лист утверждения;

– Ведомость техно-рабочего проекта.

3.1.4.5 Этап 5. Ввод в действие аппаратных и программных компонентов средств защиты на объектах Заказчика, проведение предварительных испытаний, опытной эксплуатации и приемочных испытаний

Работы по вводу в действие программных и программно-аппаратных средств должны быть выполнены в соответствии с требованиями разработанного технического проекта на систему защиты информации.

Ввод в действие средств защиты информации должно включать следующие работы:

– подготовка объекта информатизации к внедрению программных и программно-аппаратных средств;

– установка средств защиты информации на объектах Заказчика после поставки средств защиты информации;

– настройка средств защиты информации в соответствии с заявленной категорией и классом защищенности;

– предварительные испытания объекта информатизации;

– опытная эксплуатация объекта информатизации;

– приемочные испытания объекта информатизации.

Все испытания проводятся в соответствии с программой и методикой испытаний, разработанной на этапе 4 (Разработка комплекта документации технического проекта). Программа и методика испытаний должна устанавливать необходимый и достаточный объем испытаний и охватывать реализуемую функциональность и виды обеспечений.

Приемка системы проводится комиссией в составе уполномоченных представителей Заказчика и Исполнителя на соответствие требованиями настоящего ТЗ и разработанного Частного технического задания на систему защиты информации.

Система считается прошедшей предварительные испытания, если контрольный список вопросов не менее чем на 80% заполнен положительными ответами. Недостатки устраняются Исполнителем в процессе опытно-промышленной эксплуатации системы. По результатам предварительных испытаний по согласованию между Исполнителем и Заказчиком могут быть внесены изменения в техническую документацию на систему.

Система считается прошедшей приемочные испытания, если контрольный список вопросов не менее чем на 95% заполнен положительными ответами. Недостатки устраняются Исполнителем в процессе эксплуатации системы в порядке гарантийного обслуживания системы. По результатам предварительных испытаний по согласованию между Исполнителем и Заказчиком могут быть внесены изменения в техническую документацию на систему.

Решение о присвоении ответа контрольному вопросу принимается простым большинством голосов членов приемочной комиссии.

После проведения данного этапа оказанных услуг должны быть достигнуты следующие результаты:

– выполнена установка и настройка средств защиты информации на объектах Заказчика.

– подписаны акты установки средств защиты на объекты Заказчика;

– заполнены протоколы испытаний;

– подписан акт приемки системы в опытную эксплуатацию;

– подписан акт сдачи-приемки оказанных услуг по проверке в режиме опытной эксплуатации;

– подписан акт приемки системы в промышленную эксплуатацию.

3.1.4.6 Этап 6. Разработка технического паспорта. Разрабатываются следующие документы:

– Технический паспорт;

– Проект приказа о вводе в постоянную эксплуатацию.

3.1.4.7 Этап 7. Аттестация АСЗИ Заказчика на соответствие требованиям по защите информации по классу защищенности от НСД 1Г в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа

к информации. Классификация автоматизированных систем и требования по защите информации» ФСТЭК России, а также по требованиям безопасности к определенному в процессе выполнения услуг уровню защищенности персональных данных.

Задачей аттестационных испытаний АСЗИ является оценка соответствия требованиям безопасности информации, выполнение которых позволяет защитить информацию от утечки от несанкционированного доступа и от специальных воздействий на нее и ее носители.

При проведении аттестационных испытаний применяются следующие методы проверок и испытаний:

– экспертно-документальный метод предусматривает проверку соответствия подсистем обеспечения информационной безопасности ИС установленным требованиям безопасности информации на основании экспертной оценки полноты и достаточности необходимых мер защиты информации в представленных документах, а также на основании соответствия реальных условий эксплуатации требованиям к размещению, монтажу и эксплуатации технических средств.

– проверка функций или комплекса функций защиты информации от несанкционированного доступа с помощью инструментальных средств контроля, а также путем пробного запуска средств защиты информации от несанкционированного доступа и наблюдения за выполнением их функций;

– проверка соответствия примененных параметров настройки элементов подсистем АСЗИ требованиям безопасности информации;

– проверка реализации защиты подсистем АСЗИ от несанкционированного доступа, целостности применяемых средств защиты информации от несанкционированного доступа, в том числе с использованием специальных средств контроля эффективности защиты информации;

– проверка программной совместимости и корректности функционирования всего комплекса используемых средств вычислительной техники с продукцией, используемой в целях защиты информации;

– испытания подсистем защиты АСЗИ от несанкционированного доступа путем попыток осуществить несанкционированный доступ к тестовой защищаемой информации в обход используемой системы защиты информации в АСЗИ, в том числе с использованием специальных программных тестирующих средств.

Проверки должны выполняться в соответствии с разработанной Исполнителем Программой и методикой аттестационных испытаний АСЗИ.

Измерения и оценка защищенности осуществляются с помощью инструментальных средств контроля эффективности системы защиты информации в АСЗИ в соответствии с действующими нормативными и методическими документами по защите информации.

Проверка и испытания комплекса функций защиты информации от несанкционированного доступа проводятся для программно-технической среды в целом, в соответствии с действующими документами по защите информации от несанкционированного доступа.

Проверка соответствия системы защиты информации в АСЗИ требованиям безопасности информации проводится на основании анализа общих результатов испытаний и выявленных в процессе испытаний недостатков и нарушений.

В случае выявления по результатам испытаний несоответствия системы защиты информации в АСЗИ установленным требованиям по защите информации комиссия может рассмотреть возможность оперативного устранения выявленных недостатков и нарушений. При этом могут рекомендоваться следующие меры:

– доработка организационно-распорядительной документации;

– исключение отдельных технических средств из состава АСЗИ;

– применение дополнительных организационных и технических мер защиты;

– применение дополнительных сертифицированных средств защиты информации.

По окончании вышеперечисленных оказанных услуг Исполнителем разрабатываются следующая отчетная документация:

– протокол испытаний системы защиты информации в АСЗИ;

– заключение по результатам испытаний системы защиты информации в АСЗИ;

– аттестат соответствия системы защиты информации в АСЗИ (в случае положительного заключения).

Подраздел 3.2 Требования к качеству оказываемых услуг

3.2.1 Оказываемые услуги и поставляемые средства защиты должны соответствовать следующим документам:

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных»;

– Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– 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»;

– Приказ ФСБ России № 378 от 10 июля 2014 года «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 ФАПСИ от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

– «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», Решение председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 г.;

– «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержден Решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 г.;

– «Руководящий документ. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», Решение председателя Гостехкомиссии России от 25.07.1997 г.;

– «Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей»,

Приказ председателя Государственной технической комиссии при Президенте Российской Федерации от 04.06.1999 г. №114;

– ГОСТ РО 0043-003-2012. Разработан ФСТЭК России, принят и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 17.04.2012 г. №2-ст РО;

– ГОСТ РО 0043-004-2013. Разработан ФАУ «ГНИИИ ПТЗИ ФСТЭК России», принят и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 12.04.2013 г. №1-ст РО;

– ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения;

– Федеральный закон Российской Федерации от 29.07.2004 г. №98-ФЗ «О коммерческой тайне»;

– Постановление Правительства Российской Федерации от 03.11.1994 г. №1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

– «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения», утвержден Решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 г.

– «Руководящий документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержден Приказом Государственной технической комиссии при Президенте Российской Федерации от 30.08.2002 г. № 282-дсп;

– «Единые отраслевые методические указания по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях» утверждены приказом АО «Концерн Росэнергоатом» от 09.03.2021 №9/01/18-П-ДСП.

Подраздел 3.3 Требования к гарантийным обязательствам оказываемых услуг

3.3.1 Результаты оказанных услуг Исполнителя должны обеспечиваться гарантией на срок не менее 3 лет, в течение которого гарантируется надлежащее качество оказанных услуг, соответствие их техническим требованиям.

3.3.2 Исполнитель гарантирует, что специалисты, обладают достаточной квалификацией, опытом и имеют все сертификаты, требуемые производителями для оказания услуг с оборудованием и программным обеспечением.

Подраздел 3.4 Требования к конфиденциальности

3.4.1 Сведения, относящиеся к предмету оказания услуг, предназначены исключительно для Исполнителя и Заказчика и не могут быть полностью или частично переданы (опубликованы, разглашены) третьим лицам или использованы каким-либо иным способом с участием третьих лиц без согласия Исполнителя и Заказчика, за исключением случаев, установленных законодательством Российской Федерации.

3.4.2 Взаимодействие Исполнителя и Заказчика, касающиеся порядка обмена, обработки, хранения, распространения и предоставления доступа к информации должно осуществляться в соответствии с Политикой информационной безопасности АО «Концерн Росэнергоатом» и Порядком предоставления доступа к информационным ресурсам АО «Концерн Росэнергоатом».

Подраздел 3.5 Требования к безопасности оказания услуг и безопасности результата оказанных услуг

3.5.1 При оказании услуг Исполнитель обеспечивает безопасность существующих данных (сохранность хранимой в них информации).

3.5.2 В ходе оказания услуг Исполнитель обязан обеспечить соблюдение общественного порядка, установленных правил пожарной и электробезопасности, а также правил техники безопасности при оказании услуг на территории Заказчика. Услуги должны быть оказаны без причинения вреда здоровью граждан, имуществу юридических и физических лиц.
Подраздел 3.6 Требования по обучению персонала заказчика
3.6.1 Исполнитель проводит инструктаж Заказчика.
Подраздел 3.7 Требования к Исполнителю и к составу технического предложения участника
3.7.1 Техническое предложение участника должно подробно описывать подход исполнителя к порядку оказания услуг по настоящему техническому заданию, с указанием методов и технологий, используемых для качественного выполнения работ, содержать конкретные наименования оборудования и ПО, предлагаемого к поставке в соответствии с настоящими требованиями. 3.7.2 Исполнитель должен обладать необходимыми лицензиями и свидетельствами о допуске: – Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации; – Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания 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);
Подраздел 3.8 Специальные требования
Требования не предъявляются.

РАЗДЕЛ 4. РЕЗУЛЬТАТ ОКАЗАННЫХ УСЛУГ

Подраздел 4.1 Описание конечного результата оказанных услуг
4.1.1 По завершению оказанных услуг Заказчик получит следующие значимые результаты: – проведено обследование объектов информатизации Заказчика, оценка соответствия АСЗИ и имеющейся системы защиты требованиям по защите информации (как организационным, так и техническим); – произведена классификация АСЗИ как информационной системы по установленному классу защищенности и персональных данных по соответствующему уровню защиты; – разработана модель угроз и модель нарушителя информационной безопасности, и частное техническое задание на АСЗИ; – разработаны и реализованы необходимые дополнительные организационные и технические решения по защите информации, отвечающие требованиям по защите информации, регламентированным действующим законодательством, нормативно-

методическими документами ФСТЭК России и Отраслевыми требованиями по информационной безопасности Госкорпорации «Росатом»;

– оказаны услуги по внедрению средств защиты информации в соответствии с техническими решениями;

– выполнена подготовка к проведению аттестационных испытаний АСЗИ и комплекта документов, необходимых для представления АСЗИ Заказчика к аттестационным испытаниям на соответствие требованиям безопасности информации по установленному классу защищенности в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» ФСТЭК России, а также по требованиям безопасности к определенному в процессе выполнения услуг уровню защищенности персональных данных;

– проведены аттестационные испытания АСЗИ Заказчика, и выдан аттестат соответствия требованиям по безопасности информации по установленному классу защищенности в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» ФСТЭК России, а также по требованиям безопасности к определенному в процессе выполнения услуг уровню защищенности персональных данных.

– проведен обязательный ежегодный инструментальный контроль аттестованной автоматизированной системы Заказчика.

Подраздел 4.2 Требования по приемке услуг и срокам выполнения работ

Исполнитель осуществляет сдачу оказанных услуг по этапам. В пределах сроков завершения отдельных этапов Услуг, Исполнитель обеспечивает получение Заказчиком на все оказанные Услуги по соответствующему этапу подписанного со своей Стороны Акта об оказании услуг, отчета об оказанных услугах, оригинала счета и счета-фактуры, оформленных надлежащим образом, документов, подтверждающих полномочия лица на подписание указанных выше документов от имени Исполнителя (приказы, доверенности и т.д.), заверенных Исполнителем надлежащим образом (с надписью «Копия верна», подписью уполномоченного лица и печатью Исполнителя), а также необходимых документов, предусмотренных в Техническом задании. При этом Стороны договорились, что счет-фактура оформляется в соответствии с действующим законодательством РФ и выставляется только на бумажном носителе.

Для обеспечения соответствия внедряемой СЗИ АСЗИ требованиям настоящего Технического задания необходимо предусмотреть на стадии ввода в действие СЗИ АСЗИ следующие виды испытаний:

– предварительные испытания;

– опытная эксплуатация;

– приемочные испытания.

Испытания проводятся в соответствии с Программой и методикой испытаний, разработанной до начала испытаний. Программа и методика испытаний должна устанавливать необходимый и достаточный объем испытаний и охватывать реализуемую функциональность и виды обеспечений.

Приемка системы проводится комиссией в составе уполномоченных представителей Заказчика и Исполнителя на соответствие требованиями настоящего Технического задания.

4.2.1 Предварительные испытания.

Предварительные испытания проводятся в соответствии с разработанной Программой и методикой испытаний.

По результатам предварительных испытаний Исполнителем предоставляется следующая документация: Акт приемки в опытную эксплуатацию СЗИ АСЗИ.

4.2.2 Опытная эксплуатация.

Опытная эксплуатация СЗИ АСЗИ проводится с целью определения фактических значений количественных и качественных характеристик и готовности персонала к оказанию услуг в условиях функционирования СЗИ АСЗИ.

При необходимости изменения проектной и эксплуатационной документации, возникшие в период опытной эксплуатации, вносятся в нее без выпуска извещения на изменение и утверждаются Заказчиком и Исполнителем.

Условием начала опытной эксплуатации является утверждение Заказчиком и Исполнителем Акта ввода в опытную эксплуатацию СЗИ АСЗИ.

На этапе опытной эксплуатации Исполнителем предоставляется следующая документация:

1. Рабочий журнал опытной эксплуатации с выявленными в период проведения опытной эксплуатации замечаниями, в котором фиксируются:

– произошедшие сбои и/или отказы, ложные срабатывания компонентов СЗИ АСЗИ;

– дополнительные настройки компонентов СЗИ АСЗИ, вносимые по итогам отладки конфигурации и анализа регистрируемых событий.

2. Протокол об исправлении ошибок.

Опытная эксплуатация должна быть проведена в течение не более 2-х недель с даты проведения предварительных испытаний.

4.2.3 Приемочные испытания.

Приемочные испытания проводятся в соответствии с разработанной Программой и методикой испытаний.

По результатам приемочных испытаний Исполнителем предоставляется следующая документация:

1. Протокол приемочных испытаний;

2. Акт приемки в промышленную эксплуатацию СЗИ АСЗИ.

Протокол должен содержать следующие разделы:

– назначение испытаний;

– состав технических и программных средств, используемых при испытаниях;

– указания методик, в соответствии с которыми проводились испытания;

– условия проведения испытаний и характеристики исходных данных;

– оцениваемые показатели, результаты испытаний и оценка выполнения программы испытаний;

– обобщенные результаты испытаний;

– выводы о результатах испытаний и соответствии созданной системы требованиям Технического задания.

По результатам приемочных испытаний Исполнителем предоставляется Акт приемки в промышленную эксплуатацию СЗИ АСЗИ с Протоколом приемочных испытаний, утверждаемый Заказчиком и Исполнителем.

4.2.4 Приемочная комиссия.

Приемочная комиссия должна состоять из сотрудников Заказчика и Исполнителя.

Подраздел 4.3 Требования по передаче Заказчику технических и иных документов (оформление результатов оказанных услуг)

4.3.1 По завершению оказанных услуг, Исполнителем должен быть передан Заказчику следующий комплект документов:

4.3.1.1 В рамках выполнения Этапа 1 (Обследование объектов информатизации Заказчика и классификация АСЗИ Заказчика):

– Отчет об обследовании, содержащий актуальную информацию о текущем состоянии АС.
– Проект акта классификации АС, в том числе определение требуемого уровня защищенности ПДн, обрабатываемых в АС.

4.3.1.2 В рамках выполнения Этапа 2 (Разработка модели угроз и модели нарушителя информационной безопасности):

– Проект модели угроз информационной безопасности и модели нарушителя информационной безопасности.

4. 3.1.3 В рамках выполнения Этапа 3 (Разработка организационно-распорядительной документации):

4. 3.1.3.1 Документы, определяющие состояние автоматизированной системы:

Должны быть разработаны следующие проекты документов:

– Приказ об определении границ контролируемой зоны;
– Технический паспорт;
– Перечень защищаемых ресурсов;
– Приказ об определении ответственных должностных лиц за выполнение требований по защите информации;
– Должностные обязанности лиц, ответственных за выполнение требований по защите информации;
– Положение о порядке организации и проведении работ по защите конфиденциальной информации;
– Таблица разграничения доступа (матрица доступа);
– Описание технологического процесса обработки информации;
– Инструкция администратора информационной безопасности;
– Инструкция пользователя;
– Проект Приказа о вводе в эксплуатацию АСЗИ.

4.3.1.3.2 Журналы, перечни и списки:

Должны быть разработаны следующие проекты документов:

– Журнал учета инцидентов информационной безопасности;
– Журнал учета машинных носителей, предназначенных для хранения конфиденциальной информации;
– Журнал регистрации печати конфиденциальной информации;
– Журналы учета паролей администраторов АС;
– Перечень правил фильтрации межсетевых экранов;
– Список пользователей, допущенных к обработке конфиденциальной информации;
– Список пользователей, допущенных в помещения, где располагаются технические средства АС.

Состав организационно-распорядительной документации может быть актуализирован на этапе разработки требований на создание АСЗИ.

4.3.1.4 В рамках выполнения Этапа 4 (Разработка комплекта документации технического проекта):

– Ведомость технического проекта;
– Пояснительная записка к техническому проекту;
– Лист утверждения технического проекта.

4.3.1.5 В рамках выполнения Этапа 5 (Разработка комплекта эксплуатационной и рабочей документации):

– Руководство пользователя;
– Программа и методика испытаний.

4.3.1.6 В рамках выполнения Этапа 6 (Ввод в действие (настройка) аппаратных и программных компонентов средств защиты на объектах Заказчика, проведение предварительных испытаний, опытной эксплуатации и приемочных испытаний):

- акт установки и настройки средств защиты;
- протокол предварительных испытаний;
- акт приемки системы в опытную эксплуатацию;
- рабочий журнал опытной эксплуатации;
- акт сдачи-приемки оказанных услуг по проверке в режиме опытной эксплуатации;
- протокол приемочных испытаний;
- акт приемки системы в промышленную эксплуатацию.

4.3.1.7 В рамках выполнения Этапа 7 (Аттестация АСЗИ Заказчика на соответствие требованиям по защите информации, а также по требованиям безопасности к определенному в процессе выполнения услуг уровню защищенности персональных данных):

- программа и методики аттестационных испытаний;
- протокол испытаний системы защиты информации в АСЗИ;
- заключение по результатам испытаний системы защиты информации в АСЗИ;
- аттестат соответствия системы защиты информации в АСЗИ.

4.3.1.8 В рамках выполнения Этапа 8 (Проведение обязательного ежегодного инструментального контроля аттестованной автоматизированной системы Заказчика»):

- протокол контрольных испытаний;
- заключение о ежегодном контроле.

Оформление результатов услуг осуществляется в соответствии с ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (http://docs.cntd.ru/document/gost-34-201-89).

Программа и методика испытаний разрабатывается и оформляется с учетом положений ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

Отчетные документы по этапам 1, 2, 3 предъявляются в одном экземпляре электронном виде на CD-ROM.

Отчетные документы по этапам 4, 5, 6, 7, 8 предъявляются в одном экземпляре на бумажном носителе.

Документация в электронном виде предоставляется Заказчику в формате:

- текстовые документы – Microsoft Word;
- схемы, рисунки и другие графические материалы – Microsoft Visio.

РАЗДЕЛ 5. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБУЧЕНИЮ ПЕРСОНАЛА ЗАКАЗЧИКА

Не предъявляется.

РАЗДЕЛ 6. ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

№ п/п	Сокращение	Расшифровка сокращения
1	АРМ	Автоматизированное рабочее место
2	АС	Автоматизированная система

3	АСЗИ	Автоматизированная система в защищенном исполнении
4	ИБ	Информационная безопасность
5	ИТ	Информационные технологии
6	ИС	Информационная система
7	НПА	Нормативно-правовой акт
8	НСД	Несанкционированный доступ
9	ОРД	Организационно-распорядительная документация
10	ОС	Операционная система
11	ПО	Программное обеспечение
12	СЗИ	Система защиты информации
13	СрЗИ	Средства защиты информации
14	СКЗИ	Средство криптографической защиты информации
15	ФСБ	Федеральная служба безопасности
16	ФСТЭК	Федеральная служба по техническому и экспортному контролю
17	КТС	Комплекс технических средств

Советник по безопасности _____ Г.А. Егерев