УТВЕРЖДАЮ
Заместитель директора по безопасности
_____ **А.А. Корабельников**
«25» 02 **2013 г.**

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

на создание автоматизированной системы в защищенном исполнении (АСЗИ)

1. Наименование закупки:

создание автоматизированной системы в защищенном исполнении (АСЗИ)

2. Технические требования к поставке товара/выполнению работ:

- **ЦЕЛЬ И ЗАДАЧИ РАБОТЫ**

Целью выполнения работ является приведение предприятия к соответствию отраслевым требованиям по информационной безопасности Госкорпорации «Росатом».
При выполнении работ должны быть решены следующие задачи:

- проведено обследование объекта информатизации;
- проведена адаптация отраслевых типовых организационно-распорядительных и нормативно-методических документов Госкорпорации «Росатом»;
- проведена адаптация отраслевых типовых технических решений по обеспечению информационной безопасности;
- выполнена поставка средств защиты информации;
- проведены работы по внедрению средств защиты информации в соответствии с адаптированными техническими решениями;
- подготовлен комплект документов, необходимых для представления АСЗИ предприятия к аттестации на соответствие требованиям безопасности информации по классу защищенности 1Г;
- проведена аттестация АСЗИ организации по классу защищенности 1Г в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» Гостехкомиссии России (ФСТЭК России).

- **ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ ОБСЛЕДОВАНИЯ ОБЪЕКТА ИНФОРМАТИЗАЦИИ**

Целью проведения работ по обследованию объекта информатизации является оценка текущего состояния мер по обеспечению ИБ информационных ресурсов объекта информатизации и определение необходимых мероприятий и средств защиты

информации для повышения уровня безопасности информационных ресурсов объекта информатизации.
Работы по обследованию объекта информатизации должны включать:

- сбор исходных данных об объекте информатизации, мерах по обеспечению ИБ информационных ресурсов объекта информатизации и их последующий анализ;
- разработку Отчета об обследовании объекта информатизации;
- разработку рекомендаций по подготовке объекта информатизации к внедрению средств защиты информации (реализация рекомендаций выполняется силами Заказчика);
- определение актуальных угроз и актуальных нарушителей ИБ АСЗИ предприятия;
- проведение классификации АСЗИ предприятия;
- разработка требований к СОИБ АСЗИ предприятия.

Результатом работ по обследованию АСЗИ предприятия должен являться следующий комплект документации:

- Отчет об обследовании АСЗИ предприятия;
- Модель угроз и модель нарушителя информационной безопасности АСЗИ предприятия;
- Акт классификации АСЗИ предприятия по требованиям безопасности информации;
- Техническое задание на создание СОИБ АСЗИ предприятия.

- **ТРЕБОВАНИЯ К АДАПТАЦИИ ОТРАСЛЕВЫХ ТИПОВЫХ НОРМАТИВНО-МЕТОДИЧЕСКИХ И ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫХ ДОКУМЕНТОВ**

Целью адаптации типовых организационно-распорядительных и нормативно-методических документов является формирование комплекта руководящих документов в области ИБ для организации, синхронизированных с едиными отраслевыми принципами и подходами по обеспечению безопасности информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.
Исходными данными для адаптации организационно-распорядительных и нормативно-методических документов являются типовые документы и методические указания по адаптации (перечень представлен в Приложении 1).
Результатом работ по адаптации должен являться адаптированный перечень следующих документов:

Набор (комплект) Частных Политик информационной безопасности предприятия:

- Политика антивирусной защиты;
- Политика парольной защиты;
- Политика использования сервиса электронной почты;
- Политика удаленного доступа;
- Политика использования носителей информации и мобильных устройств;
- Политика использования ресурсов сети Интернет;
- Политика предоставления доступа к информационным активам;

- Политика обеспечения непрерывности деятельности;
- Политика управления инцидентами;
- Политика контроля защищенности информационных активов;
- Политика безопасности информационной среды и системных ресурсов;
- Политика использования средств криптографической защиты;
- Политика работы с конфиденциальной информацией;
- Политика безопасности коммуникаций.

Набор (комплект) Процедур менеджмента информационной безопасности предприятия:

- Процедура учета носителей информации и мобильных устройств;
- Процедура утилизации носителей информации;
- Процедура предоставления доступа к внешним сетевым ресурсам;
- Процедура предоставления доступа к информационным ресурсам;
- Процедура управления учетными записями в информационных системах;
- Процедура классификации информационных ресурсов;
- Процедура идентификации, анализа и реагирования на инциденты информационной безопасности;
- Процедура расследования инцидентов информационной безопасности;
- Процедура проверки соответствия информационных систем и компонентов ИТ-инфраструктуры требованиям безопасности;
- Положение о режиме защиты коммерческой тайны;
- Положение о защите персональных данных;
- Положение о защите служебной информации ограниченного распространения;
- Процедура получения и передачи конфиденциальной информации;
- Процедура проведения внутреннего аудита по информационной безопасности.

Набор (комплект) Процедур управления непрерывностью бизнеса предприятия:

- Процедура резервного копирования;
- Процедура проведения тестирования корректности резервных копий;
- Процедура восстановления резервных копий.

Набор (комплект) Процедур обеспечения информационной безопасности предприятия:

- Инструкция по антивирусной защите;
- Памятка по информационной безопасности пользователя информационной системы;
- Инструкция по безопасной работе с электронной почтой;
- Процедура предоставления удаленного доступа к информационным ресурсам;
- Инструкция пользователя по безопасной работе в сети Интернет;

- Процедура учета СКЗИ, эксплуатационной и технической документации к ним;
- Процедура контроля использования СКЗИ;
- Процедура учета лиц, допущенных к работе с СКЗИ;
- Инструкция по работе с коммерческой тайной;
- Инструкция по работе с персональными данными;
- Инструкция по работе со служебной информацией ограниченного распространения;
- Инструкция администратора информационной безопасности.

Положение о порядке организации и выполнения работ по обеспечению информационной безопасности на предприятии

Все типовые документы и методики адаптации предоставляются Центральным аппаратом Госкорпорации «Росатом» по запросу.

- **ТРЕБОВАНИЯ К АДАПТАЦИИ ОТРАСЛЕВЫХ ТИПОВЫХ БАЗОВЫХ ТЕХНИЧЕСКИХ РЕШЕНИЙ**

Целью адаптации отраслевых типовых базовых технических решений является формирование проектной документации на СОИБ АСЗИ предприятия, синхронизированной с едиными отраслевыми техническими принципами и подходами по обеспечению безопасности информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

В рамках адаптации типовых базовых технических решений должны быть разработаны следующие проектные документы на СОИБ АСЗИ предприятия:

- Пояснительная записка к техническому проекту СОИБ АСЗИ предприятия;
- Спецификация на поставку программно-технических средств СОИБ АСЗИ предприятия;
- Инструкция по эксплуатации КТС;
- Руководство пользователя;
- Программа и методика испытаний СОИБ АСЗИ предприятия.

В состав СОИБ АСЗИ предприятия должны входить следующие подсистемы информационной безопасности:

- подсистема межсетевого экранирования;
- подсистема защиты каналов связи;
- подсистема обнаружения и предотвращения вторжений;
- подсистема антивирусной защиты;
- подсистема защищенного доступа к ресурсам сети Интернет;
- подсистемы обнаружения утечек конфиденциальной информации.
- подсистема анализа защищенности;
- подсистема мониторинга событий информационной безопасности;
- подсистема защиты рабочих станций от несанкционированного доступа.

Набор подсистем ИБ может быть уточнен после разработки Модели угроз и модели нарушителя ИБ АСЗИ предприятия.

Все типовые документы и методики адаптации предоставляются Центральным аппаратом Госкорпорации «Росатома» по запросу. Перечень дополнительных документов может быть уточнен на этапе подготовки конкурсного ТЗ.

- **ТРЕБОВАНИЯ К РАБОТАМ ПО ПОСТАВКЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

Поставка средств защиты информации должна быть выполнена согласно разработанной Исполнителем и утверждённой Заказчиком Спецификации программно-технических средств СОИБ АСЗИ предприятия.

Поставка программного обеспечения должна осуществляться в электронном виде на съемных носителях.

- **ТРЕБОВАНИЯ К РАБОТАМ ПО ВНЕДРЕНИЮ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ СОИБ АСЗИ ПРЕДПРИЯТИЯ**

Работы по внедрению средств защиты информации должны быть выполнены в рамках адаптированного и согласованного проектного решения на АСЗИ предприятия.
Работы по внедрению средств защиты информации СОИБ АСЗИ предприятия должны включать:

- подготовку Заказчиком объекта информатизации к внедрению средств защиты информации СОИБ АСЗИ предприятия;
- пусконаладочные работы;
- предварительные испытания СОИБ АСЗИ предприятия;
- опытную эксплуатацию СОИБ АСЗИ предприятия;
- приемочные испытания СОИБ АСЗИ предприятия

Для выполнения работ по внедрению подсистем СОИБ АСЗИ организации у Исполнителя должны быть необходимые лицензии, ресурсы, знания и опыт проведения аналогичных работ.

- **ТРЕБОВАНИЯ К ПОДГОТОВКЕ ДОКУМЕНТОВ ДЛЯ ПРЕДОСТАВЛЕНИЯ АСЗИ К АТТЕСТАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ**

В рамках подготовки АСЗИ предприятия к аттестации по требованиям безопасности информации должен быть разработан следующий комплект документов:

- Матрица доступа к ресурсам АСЗИ предприятия;проект документа «Перечень конфиденциальной информации, обрабатываемой в АСЗИ предприятия»;
- проект документа «Перечень лиц, допущенных к обработке конфиденциальной информации»;
- проект документа «Перечень лиц, допущенных в помещения, в которых располагаются технические средства АСЗИ предприятия»;
- проект документа «Акт классификации АСЗИ предприятия»;
- проект документа «Акт внедрения СЗИ» (при необходимости);
- Технический паспорт на АСЗИ предприятия с указанием заводских номеров оборудования;
- Описание технологического процесса обработки информации в АСЗИ предприятия;
- Положение о разрешительной системе доступа пользователей и эксплуатационного персонала АСЗИ к обрабатываемой информации;

- Проект приказа об определении подразделений и лиц, ответственных за эксплуатацию средств и мер защиты информации;
- проект Приказа о вводе АСЗИ в эксплуатацию;
- Положение о порядке организации и проведения работ по защите конфиденциальной информации;
- Инструкция администратора информационной безопасности;
- Инструкция пользователя АСЗИ;
- Журнал учета печати конфиденциальной информации;
- Журнал учета машинных носителей информации;
- Перечень правил межсетевого экранирования.

Перечень документов может быть уточнен по согласованию между Заказчиком и Исполнителем.

- **ТРЕБОВАНИЯ К РАБОТАМ ПО АТТЕСТАЦИИ АСЗИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ**

Аттестация АСЗИ предприятия по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых в АСЗИ мер и средств защиты информации.

Аттестационные испытания АСЗИ должны осуществляться аттестационной комиссией, формируемой Исполнителем, – органом по аттестации, аккредитованным ФСТЭК России. Аттестационные испытания проводятся по программе и методике испытаний и в соответствии с Положением по аттестации объектов информатизации.

Под аттестацией АСЗИ понимается комплекс организационно-технических мероприятий, в результате которых специальным документом – Аттестатом соответствия – подтверждается, что АСЗИ соответствуют требованиям стандартов и нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Аттестация АСЗИ по требованиям безопасности информации проводится в 2 этапа:

1. Подготовка и проведение аттестационных испытаний на площадке размещения АСЗИ;
2. Подготовка отчетных документов по результатам проведенных испытаний.

На первом этапе должны быть проведены следующие работы:

– проверка состояния технологического процесса автоматизированной обработки;

– проверка АСЗИ на соответствие организационно-техническим требованиям по защите информации;

– испытания АСЗИ на соответствие требованиям установленного класса защищенности;

– инструментальный анализ защищенности АСЗИ с применением сканера защищенности (сканирование должно проводиться с применение сертифицированных средств защиты).

На втором этапе работ подготавливается пакет отчетных документов в составе:

- протокол проведения аттестационных испытаний;
- заключение по результатам проведенных испытаний;
- аттестат соответствия (в случае положительного Заключения).

Для выполнения работ по проведению аттестации АСЗИ предприятия у Исполнителя должны быть необходимые лицензии, ресурсы, знания и опыт проведения аналогичных работ.

3. **Требования к упаковке и маркировке (для товаров)**

- Упаковка должно полностью обеспечивать условия транспортировки и хранения, предъявляемые к данному виду товара.

4. **Требования к гарантии качества**

- Гарантийный срок службы ПО не менее 12 месяцев.
- Поставщик должен обеспечить техническую поддержку ПО в течение гарантийного срока.
- Поставщик должен обладать всеми необходимыми лицензиями или свидетельствами о допуске на поставку ПО в соответствии с действующим законодательством Российской Федерации.
- Должен представить копии дилерского или дистрибьюторского договора, документа от изготовителя указанного в заявке ПО, подтверждающее право участника на законных основаниях предлагать такое ПО.

5. **Требования к объему технической документации:**

Предпроектное обследование:

- Отчет об обследовании.
- Техническое задание.
- Пояснительная записка к эскизному проекту.

Адаптация комплекта технических решений:

- Технорабочий проект (пояснительная записка).
- Спецификация оборудования.
- Программа и методика испытаний.
- Инструкция по эксплуатации.

Приобретение и поставка ПО:

- Копии лицензий ФСТЭК (ФСБ) на поставляемое ПО;
- Сертификат соответствия.
- Технический паспорт на изделие (на русском языке);
- Техническая поддержка на весь гарантийный период;
- Оформленные гарантийные талоны или аналогичные документы с указанием заводских (серийных) номеров товаров и гарантийного периода.

Комплект организационно-распорядительной документации, необходимой для аттестации АСЗИ:

- Технический паспорт АСЗИ.
- Инструкция по эксплуатации.
- Техническое описание;

- Приказы, журналы, списки.
- Акт классификации.

Внедрение подсистем ИБ:

- Акт внедрения подсистем ИБ.
- Акты приемки подсистем ИБ в опытную эксплуатацию.

Подготовка комплекта организационно-распорядительной документации к аттестации АСЗИ:

- Комплект организационно-распорядительной документации.

Приемочные испытания :

- Акт о проведении и результатах испытания.

Ввод АСЗИ в опытную эксплуатацию:

- Акт о вводе в опытную эксплуатацию.

Проведение аттестации АСЗИ по классу 1Г:

- Аттестат ФСТЭК по классу защищенности 1Г, комплект документов.

Ввод АСЗИ в промышленную эксплуатацию:

- Акт ввода АСЗИ в промышленную эксплуатацию.

6. Место поставки товара/выполнения работ/оказания услуг:

ул. Орджоникидзе д.21, г. Подольск, Московской обл., ОАО ОКБ «ГИДРОПРЕСС»

7. Срок поставки товара/выполнения работ/оказания услуг:

- Поставка, не более 2-х недель с даты заключения договора;
- Выполнения работ, не более 50 дней с даты заключения договора.

Подписи:

Начальник отдела 7.08 — В.В. Черняк

25.02.15

Исполнитель: В.В. Черняк Тел. 29-68