|  |  |
| --- | --- |
| Согласовано:  *Заместитель генерального директора*  *по производству*  *ООО «Интер РАО - ИТ»*  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_202\_ г. | Утверждаю:  *Генеральный директор*  *ООО «Интер РАО - ИТ»*  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 202\_ г. |

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

на оказание услуг «Проведение аттестации объектаинформатизации по требованиям безопасности информации» в рамках проекта «Создание типовой тиражной системы Электронный архив (далее – ТТС ЭА)»

1. **НАИМЕНОВАНИЕ УСЛУГ (НОМЕНКЛАТУРА) И ПЕРЕЧЕНЬ ОБЪЕКТОВ, НА КОТОРЫХ БУДУТ ОКАЗЫВАТЬСЯ УСЛУГИ**
   1. Полное наименование услуг и их условное обозначение

**Полное наименование услуг:** Услуги по проведению аттестации объекта информатизации по требованиям безопасности информации» в рамках проекта «Создание типовой тиражной системы Электронный архив (далее – ТТС ЭА)». Организационный объем работ отражен в Приложении № 1 к настоящему Техническому заданию.

**Условное обозначение услуги:** Оказание услуг по аттестации ОИ.

* 1. **Плановая стоимость закупки составляет:** 1 440 000,00 (Один миллион четыреста сорок тысяч) рублей 00 копеек без учета НДС.
  2. **Место оказания услуг:** Подрядчик оказывает услуги на территории ООО «Интер РАО – ИТ» по адресу: г. Москва, ул. Большая Пироговская, д. 27, стр. 3а

1. **ОБЩИЕ ТРЕБОВАНИЯ**
   1. Основание для оказания услуг

Целью закупки является выбор подрядчика для оказания услуг по проведению аттестации объекта информатизации по требованиям безопасности информации» в рамках проекта «Создание типовой тиражной системы Электронный архив (далее – ТТС ЭА)». Закупка осуществляется в соответствии с решением заседания Управляющего комитета проекта (протокол от 10.07.2020 №АД/2) «О рассмотрении запроса на изменение №5 паспорта проекта «Создание Типовой тиражной системы Электронный архив (далее -ТТС ЭА)».

* 1. Требования к срокам оказания услуг

**2.2.1.** Дата начала оказания услуг – с момента заключения договора. Окончание оказания услуг – не позднее 2-х месяцев, с момента заключения договора.

**2.2.2**. Подрядчик вправе оказать услуги досрочно, а Заказчик вправе принять результат оказания услуг раньше срока, установленного договором, и оплатить стоимость оказанных услуг.

* 1. Нормативные требования к качеству предоставления услуг, их результату.

**2.3.1**. Порядок оформления и предоставления Заказчику результатов оказанных услуг определяется Договором и настоящим документом (пункт 8 и п. 6 Приложения № 1 к Техническому заданию).

Услуги должны быть оказаны на основании следующей документации, перечисленной ниже:

* 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»;
* Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
* Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
* Постановление Правительства РФ от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию 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)»;
* Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Постановление Правительства РФ от 3 февраля 2012 года № 79 «Об утверждении положения о лицензировании деятельности по технической защите конфиденциальной информации»;
* 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»;
* Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России, 15 февраля 2008 г.;
* Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России 14 февраля 2008 г.;
* Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 г. Москва "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";
* Положение по аттестации объектов информатизации по требованиям безопасности информации, Гостехкомиссия России, 1994 г;
* РД «Защита от НСД к информации», ч. 1 «Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларируемых возможностей», Гостехкомиссия России, 1999 г.;
* ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
* ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплексность и обозначение документов при создании автоматизированных систем»;
* ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
* ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
* ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»;
* ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
* ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»;
* ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

**2.3.2**.В случае, если во время оказания услуг будут изменены или уточнены настройки, которые не соответствуют документации, представленной в пункте 2.3.1, то Подрядчик должен согласовать их с Заказчиком в виде протокола и внести соответствующие правки в проектную и эксплуатационную документацию. Полный перечень проектной и эксплуатационной документации приведен в пункте «5 Приложения № 1 к Техническому заданию».

1. **ТРЕБОВАНИЯ К ОКАЗАНИЮ УСЛУГ**
   1. **Объем оказываемых услуг**

Полный состав и содержание оказываемых услуг по проведению аттестации ОИ приведен в разделе «5. Приложения № 1 к Техническому заданию «Требования к составу и содержанию услуг по аттестации ОИ Заказчика по требованиям действующего законодательства РФ в сфере защиты информации».

* 1. **Требования к последовательности этапов оказания услуг.** Не требуется.
  2. **Требования к организации обеспечения оказания услуг**. Не требуется.
  3. **Требования к применяемым материалам и оборудованию.** Не требуется.

**3.5. Требования безопасности**

**3.5.1.** Подрядчик обеспечивает соблюдение своим персоналом правил внутреннего распорядка организации Заказчика, правил техники безопасности, правил противопожарного режима (безопасности).

**3.5.2**. Подрядчик несет ответственность за причиненные его персоналом убытки, связанные с конфликтами, нарушением дисциплины.

**3.5.3.** Необходимым условием оказания услуг является наличие Соглашения о конфиденциальности между Заказчиком и Подрядчиком, распространяющее свое действие на весь период оказания услуг. При отсутствии указанного Соглашения о конфиденциальности последнее должно быть оформлено одновременно с Договором на оказание услуг.

**3.6. Требования к порядку подготовки и передачи Заказчику документов при оказании услуг и их завершении**

**3.6.1.** Подрядчик обязан уведомить Заказчика об окончании оказания услуг в рабочий день, следующий за датой окончания оказания услуг по настоящему Договору (до 12:00 по московскому времени), передав электронные версии документов, подтверждающие факт оказания услуг (Акт сдачи-приемки по оказанию услуг, составленный по форме, приведенной в Приложении №2 к Договору, предварительно согласованные Заказчиком результаты оказания услуг, указанные в Приложении №4 к Договору), посредством электронной связи по адресу электронной почты, указанному в Договоре.

**3.6.2.** Подрядчик обязан предоставить Заказчику оригиналы документов, подтверждающие факт оказания услуг, подписанные со стороны Подрядчика (Акт сдачи-приемки по оказанию услуг, составленный по форме, приведенной в Приложении №2 к Договору, предварительно согласованные Заказчиком результаты оказания услуг, указанные в Приложении №4 к Договору). Оригиналы документов должны быть направлены Заказчику не позднее 3 (трех) календарных дней, считая со дня окончания оказания услуг по договору, но в любом случае до 5-го числа месяца, следующего за месяцем окончания оказания услуг.

**3.6.3.** В случае непредставления необходимых документов, Заказчик уведомляет об этом Подрядчика. Подрядчик обязан в течение 3 (трех) календарных дней с момента получения данного уведомления Заказчика, но не позднее 5-го числа месяца, следующего за месяцем, в котором услуги были оказаны, представить недостающие документы Заказчику.

**3.6.4.** В случае наличия ошибок и иных неточностей в указанных документах Заказчик уведомляет об этом Подрядчика в течение 3 (трех) календарных дней с даты получения от Подрядчика документов, подтверждающих факт оказания услуг. В таком уведомлении Заказчик должен указать способ устранения ошибок и иных неточностей указанных документах. Подрядчик обязан в течение 3 (трех) календарных дней с момента получения данного уведомления от Заказчика устранить ошибки и иные неточности в таких документах и представить исправленные документы Заказчику.

**3.6.5.** Подрядчик предоставляет счет-фактуры в сроки в соответствии и в порядке, предусмотренном действующим законодательством Российской Федерации о налогах и сборах.

**3.7. Требования к гарантийный обязательствам**

**3.7.1.** Подрядчик гарантирует устранение в течение 10 (десяти) рабочих дней или возмещение Заказчику документально подтверждённых затрат на устранение всех выявленных в течение 12 (двенадцати) месяцев с момента подписания Акта сдачи-приемки по оказанию услуг, а также актов приема-передачи прав и оборудования, недостатков и недоработок в результате оказания услуг.

**3.8. Ответственность Подрядчика**

**3.8.1.** За нарушение условий Технического задания, повлекших ухудшение результата оказания услуг, Заказчик вправе потребовать безвозмездного устранения недостатков в сроки, установленные Заказчиком, либо соразмерного уменьшения стоимости услуг.

**3.8.2.** Подрядчик, не предупредивший Заказчика о необходимости выполнения дополнительных услуг, не учтенных в Техническом задании, которые могут повлиять на работоспособность системы, либо создают невозможность их завершения в срок, обязан возместить в полном объеме убытки, причиненные Заказчику.

**3.9. Требования к порядку привлечению субподрядчиков**

**3.9.1.** По письменному согласованию с Заказчиком возможно привлекать к выполнению Работ Субподрядчиков без увеличения стоимости услуг, требуемых в Техническом задании. При этом Подрядчик несет полную ответственность за действия третьих лиц, как за свои собственные, требования к квалификации Субподрядчика, такие же, как и к Подрядчику. Квалификация субподрядчика должна быть подтверждена документально.

1. **ПОРЯДОК ФОРМИРОВАНИЯ КОММЕРЧЕСКОГО ПРЕДЛОЖЕНИЯ УЧАСТНИКА ЗАКУПКИ, ОБОСНОВАНИЯ ЦЕНЫ, РАСЧЕТОВ, ПРЕДОСТАВЛЕНИЯ БАНКОВСКИХ ГАРАНТИЙ**
   * 1. Стоимость предложения Участника закупки не должна превышать предельную стоимость закупки, определенную в п.1.2. настоящего ТЗ.
     2. Порядок обоснования стоимости предложения

Участник закупки должен представить расчет стоимости оказываемых услуг, в т.ч. на основании расчета трудозатрат, затрат, связанных с задействованием оборудования, технических средств и иных ресурсов (в случае если применимо).

Расчет трудозатрат должен быть выполнен по форме, приведенной в Приложении №2 к настоящему техническому заданию.

* + 1. Требования к финансовому обеспечению

Требования, в т.ч. к предоставлению/наличию банковской гарантии не предъявляются.

1. **ТРЕБОВАНИЯ К УЧАСТНИКАМ ЗАКУПКИ**
   1. **Требования о наличии кадровых ресурсов и их квалификации**

Участник закупки должен иметь собственный квалифицированный персонал (в количестве не менее 3-х человек) с профильным образованием в области информационной безопасности (или с высшим техническим образованием, прошедший профессиональную переподготовку по специализации «Информационная безопасность»), обладающий необходимыми для исполнения задач по техническому заданию профессиональными знаниями и опытом, состоящий в штате компании на дату подачи предложения. В качестве подтверждения в составе заявки должны быть предоставлены копии дипломов и/или соответствующих свидетельств, выписка из организационно-штатного расписания, копия трудового договора и/или трудовой книжки.

Преимуществом будет являться наличие квалификации персонала Участника, подтвержденной следующими сертификатами:

* специалист, имеющий сертификат администратора VipNet;
* сертифицированный специалист по средству межсетевого экранирования Fortinet (не ниже NSE 4 Network Security Professional);
* сертифицированный специалист по средству защиты MaxPatrol SIEM.
  1. **Требования к измерительным приборам и инструментам:** не требуется

**5.3. Требования о наличии действующих разрешений, аттестаций, свидетельств СРО, лицензий:**

**5.3.1.** Участник закупки должен иметь Лицензию Федеральной службы по техническому и экспортному контролю России на право осуществления деятельности по технической защите конфиденциальной информации в части работ, предусмотренных подпунктами д (проектирование в защищенном исполнении средств и систем информатизации), е (услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации)) пункта 4 Положения, утвержденного Постановлением Правительства Российской Федерации от 03.03.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации». Требование установлено подпунктом 5 пункта 1 статьи 12 Федерального закона от 04.05.2011 № 99–ФЗ «О лицензировании отдельных видов деятельности». Подтверждается заверенной копией лицензии

**5.3.2.** Участник закупки должен иметь Лицензию Федеральной службы безопасности России на право осуществлять деятельность по разработке, производству, распространению 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) в части работ, предусмотренных пунктом 2 и пунктом 3 Перечня выполняемых работ, а именно «разработка защищенных с использованием шифровальных (криптографических) средств информационных систем», «разработка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем», составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16.04.2012 № 313. Требование установлено на основании подпункта 1 пункта 1 статьи 12 Федерального закона от 04.05.2011 № 99–ФЗ «О лицензировании отдельных видов деятельности». Подтверждается заверенной копией лицензии.

**5.4. Требования о наличии сертифицированных систем менеджмента**

Преимуществом будет являться наличие сертифицированной системы менеджмента качества в соответствии с требованиями международного стандарта ISO 9001:2008 или ГОСТ Р ИСО 9001-2015. Подтверждается заверенной копией соответствующего сертификата.

**5.4.** **Требования о наличии аккредитации в Группе «Интер РАО»**

Если участник закупки имеет аккредитацию в Группе «Интер РАО» в качестве поставщика работ, являющихся предметом настоящей закупки, необходимо приложить копию действующего Свидетельства об аккредитации в Группе «Интер РАО».

**5.5.** **Требования к опыту выполнения аналогичных работ:** Не предъявляются

**5.6**. **Требования к субподрядным организациям**

**5.6.1.** Требования, указанные в пунктах 5.1. - 5.5. применимы к привлекаемым Участниками субподрядчикам, в объеме поручаемых им оказания услуг, согласно «Плану распределения работ между генеральным подрядчиком и субподрядными организациями».

**5.6.2.** Документы, подтверждающие соответствие привлекаемых субподрядчиков требованиям, должны быть предоставлены в составе заявки Участника.

**5.7. Требования о наличии материально-технических ресурсов**

5.7.1. Требования к материально-технической базе для оказания услуг не предъявляются.

**6.** **ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ТЕХНИЧЕСКОГО ПРЕДЛОЖЕНИЯ УЧАСТНИКА ЗАКУПКИ.**

6.1. В Техническом предложении Участника закупки должна быть отражена готовность выполнения и/или соответствие Участника закупки предъявленным требованиям по каждому пункту ТЗ и Приложения №1 к настоящему ТЗ.

1. **ПРИЛОЖЕНИЯ**

Приложение № 1. Задание на оказание услуг;

Приложение № 1.1. Общие сведения об объекте информатизации;

Приложение № 2. Калькуляция трудозатрат на оказание услуг.

**Приложение №1**

к техническому заданию

**ЗАДАНИЕ НА ОКАЗАНИЕ УСЛУГ**

«Проведение аттестации объектаинформатизации по требованиям безопасности информации» в рамках проекта «Создание типовой тиражной системы Электронный архив (далее – ТТС ЭА)»

1. Принятые сокращения

|  |  |
| --- | --- |
| **АРМ** | Автоматизированное рабочее место |
| **АИС** | Автоматизированная информационная система |
| **ОИ** | Объект информатизации |
| **ИТ** | Информационные технологии |
| **ЛВС** | Локальная вычислительная сеть |
| **МЭ** | Межсетевой экран |
| **НСД** | Несанкционированный доступ (несанкционированные действия) |
| **ОС** | Операционная система |
| **ПО** | Программное обеспечение |
| **СЗИ** | Система защиты информации |
| **ТЗ** | Техническое задание |
| **ФСБ России** | Федеральная служба безопасности Российской Федерации |
| **ФСТЭК России** | Федеральная служба по техническому и экспортному контролю Российской Федерации |

* 1. Основные определения

|  |  |
| --- | --- |
| **Доступ к информации** | возможность получения информации и ее использования |
| **Информационная система персональных данных** | совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств |
| **Нарушитель безопасности информации** | физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах |
| **Несанкционированный доступ (несанкционированные действия)** | доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам |
| **Обработка персональных данных** | любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных |
| **Персональные данные** | любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) |
| **Технические средства информационной системы** | средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации |
| **Угрозы безопасности информации** | совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при ее обработке в информационной системе |
| **Целостность информации** | состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право |

1. Назначение и цели проведения аттестации ОИ
   1. Назначение

Основным назначением проведения аттестации ОИ является:

* предотвращение неправомерного доступа, копирования, предоставления или распространения информации ограниченного доступа (обеспечение конфиденциальности информации);
* исключение неправомерного уничтожения или модифицирования информации ограниченного доступа (обеспечение целостности информации);
* исключение неправомерного блокирования информации ограниченного доступа (обеспечение доступности информации);
* обеспечение соответствия требованиям действующего законодательства РФ в сфере защиты информации, содержащей персональные данные, при ее обработке в информационных системах персональных данных;
* обеспечение соответствия требованиям действующего законодательства РФ в сфере защиты конфиденциальной информации, в том числе персональных данных, от утечки по техническим каналам.
  1. Цели проведения аттестации ОИ

Основными целями проведения аттестации ОИ является:

* подтверждение реализации мероприятий по защите информации согласно разработанному техническому решению;
* разработка комплектов документов, необходимых для проведения аттестации ОИ на соответствие требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа;
* проведение аттестационных испытаний по требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа;
* формирование методологической основы проведения контрольных процедур на предмет соответствия требованиям безопасности информации при модернизации ОИ.

1. Характеристики объектов информатизации

Объектами защиты в рамках настоящего Технического задания являются:

* информация ограниченного распространения (в том числе персональные данные), содержащаяся в информационной системе персональных данных Заказчика;
* технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), на которых осуществляется обработка информации ограниченного доступа;
* общесистемное, прикладное, специальное программное обеспечение, информационные технологии;
* средства защиты информации, применяемые для защиты информации ограниченного доступа.

Услуги по созданию системы защиты информации Заказчика необходимо провести по адресу г. Москва, ул. Большая Пироговская, д. 27, Бизнес центр Луч.

Объектом информатизации, подлежащим аттестации, является информационная система персональных данных (далее- ИСПДн), состав которой приведен в настоящем Техническом задании.

1. Требования к системе защиты информации
   1. Общие требования к системе защиты информации
      1. Требования к структуре и функциям системы защиты информации

В составе модернизируемой системы защиты информации должны быть реализованы следующие меры защиты информации:

* идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
* управление доступом субъектов доступа к объектам доступа (УПД);
* ограничение программной среды (ОПС);
* защита машинных носителей информации (ЗНИ);
* регистрация событий безопасности (РСБ);
* антивирусная защита (АВЗ);
* обнаружение вторжений (СОВ);
* контроль (анализ) защищенности информации (АНЗ);
* обеспечение целостности информационной системы и информации (ОЦЛ);
* обеспечение доступности информации (ОДТ);
* защита среды виртуализации (ЗСВ);
* защита технических средств (ЗТС);
* защита информационной системы, ее средств, систем связи и передачи данных (ЗИС);
* выявление инцидентов и реагирование на них (ИНЦ);
* управление конфигурацией информационной системы и системы защиты персональных данных (УКФ).
  + 1. Требования к режимам функционирования

Режимы функционирования должны:

* обеспечивать возможность круглосуточного функционирования СЗИ;
* обеспечивать независимость функционирования средств защиты информации от изменений в организационной структуре объекта внедрения при сохранении состава и содержания выполняемых функций;
* допускать настройку и изменение конфигурации средств защиты информации без перепрограммирования;
* обеспечивать возможность изменения настроек, политик и правил доступа пользователей к средствам защиты информации при изменении ИТ-инфраструктуры, вводе новых регламентов обеспечения информационной безопасности, изменения организационно-штатной структуры Заказчика;
* обеспечивать возможность выявления причин неисправности взаимодействия с другими узлами сети, используя функции журналирования и изменения режимов работы средств защиты информации;
* обеспечить возможность модернизации ОИ в рамках добавления типовых сегментов[[1]](#footnote-1).

1. Требования к составу и содержанию услуг по аттестации ОИ Заказчика по требованиям действующего законодательства РФ в сфере защиты информации

Аттестационные испытания включают в себя:

* анализ организационной структуры, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
* определение правильности классификации, выбора и применения сертифицированных средств и системы защиты информации;
* проверку уровня подготовки кадров и распределения ответственности персонала за обеспечение выполнения требований по безопасности информации;
* проведение комплексных аттестационных испытаний в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации.

Должен быть разработан или актуализирован комплект документов, необходимый для прохождения аттестационных испытаний, в следующем составе:

* Технический паспорт на систему защиты информации (включает перечень технических средств обработки информации с серийными номерами, перечень средств защиты информации с серийными номерами и схему размещения компонентов системы защиты информации);
* Акт определения уровня защищенности персональных данных;
* Перечень защищаемых ресурсов;
* Разграничительная система допуска персонала к защищаемым ресурсам;
* Прочая документация, необходимая для проведения аттестационных мероприятий
* Программа и методики аттестационных испытаний.

При проведении аттестационных испытаний информационной системы Заказчика аттестационная комиссия должна руководствоваться требованиями следующих законодательных актов и нормативно-методических документов:

* Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;
* 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 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30.08.2002 № 282;
* «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам», Гостехкомиссия России, 2002 г.;
* Положение по аттестации объекта информатизации по требованиям безопасности информации, Гостехкомиссия России, 1994 г.

При проведении аттестационных испытаний объектов Заказчика должны использоваться следующие методы проверок и испытаний:

* Экспертно-документальный метод. Экспертно-документальный метод предусматривает проверку соответствия объекта информатизации требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации, а также соответствия реальных условий эксплуатации требованиям по выбору, размещению, монтажу и эксплуатации технических средств объекта;
* Проверка функций (комплекса функций) защиты информации от несанкционированного доступа с использованием тестирующих средств. Проверка и испытания функций или комплекса функций защиты информации от НСД с помощью тестирующих средств выполняется с применением специальных сертифицированных программных тестирующих средств, методом пробного пуска средств защиты или путем применения попыток «взлома» систем защиты информации;
* Разработка методики[[2]](#footnote-2) проверки соответствия типовых сегментов требованиям по безопасности в целях подтверждения соответствия сегменту ОИ, в отношении которого были проведены аттестационные испытания.

Аттестационные испытания проводятся в соответствии с разработанным Исполнителем и согласованным Заказчиком документом «Программа и методики аттестационных испытаний».

До проведения аттестационных испытаний Исполнителем готовится Технический паспорт ОИ и внутренние распорядительные документы, необходимые для проведения аттестации.

По результатам проведения аттестационных испытаний Исполнитель должен выдать комплект документов на ОИ Заказчика в следующем составе:

* Протоколы проведения аттестационных испытаний;
* Заключение по результатам аттестационных испытаний;
* Аттестат соответствия требованиям безопасности информации;
* Методика проверки соответствия типовых сегментов требованиям по безопасности.

1. Порядок контроля и приемки
   1. Согласование отчетных материалов

Содержание отчетных материалов согласуется на уровне специалистов Заказчика и Исполнителя исходя из требований к содержанию услуг, указанных в разделе 5. Отчетные документы, разработанные для объектов Заказчика, согласовываются и утверждаются уполномоченным сотрудником Заказчика.

Срок согласования отчетных материалов Заказчиком составляет 5 дней с момента предоставления материалов Исполнителем.

* 1. Общие требования к приемке оказанных услуг

Контроль и приемка оказанных услуг осуществляются на основании настоящего Технического задания и контракта.

Приёмка результатов оказанных услуг оформляется Актом оказания услуг. Основанием для составления и подписания Акта оказания услуг является предоставление Исполнителем согласованного с Заказчиком комплекта отчетных документов, либо (при проведении испытаний), утвержденных сторонами Актов приемки.

* 1. Требования к документированию

Виды, комплектность и содержание документов в части, определенной настоящим ТЗ, должны учитывать требования ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний» и ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

Вся разрабатываемая документация, а также штатная документация по поставляемому оборудованию и программному обеспечению должна быть выполнена на русском языке.

Документация, разрабатываемая (изменяемая) Исполнителем в рамках оказания услуг по настоящему Техническому заданию, передается Заказчику в бумажном (сброшюрованном) виде и, дополнительно, в электронном виде.

1. Требования к гарантиям качества

Гарантия должна распространяться на все виды оказанных услуг.

Гарантийный срок, в течение которого выявленные Заказчиком дефекты устраняются за счет Исполнителя – не менее 12 месяцев со дня подписания сторонами акта оказания услуг, а также актов приема-передачи прав и оборудования.

1. Требования к Исполнителю

Исполнитель, в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности», должен обладать лицензиями на следующие виды деятельности:

* Лицензия ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств;
* Лицензия ФСТЭК РФ на осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации.

|  |  |  |  |
| --- | --- | --- | --- |
| **Должность** | **Подпись** | **ФИО** | **Дата** |
| Начальник отдела эксплуатации средств и систем информационной безопасности ООО «Интер РАО – ИТ» |  | С.В. Хайло |  |

Ответственный исполнитель:

|  |  |  |  |
| --- | --- | --- | --- |
| **Должность** | **Подпись** | **ФИО** | **Дата** |
| Руководитель проектов Управления проектной деятельности |  | Е.Ю. Селиванова |  |

**Приложение № 1.1.**

к техническому заданию

**ОБЩИЕ СВЕДЕНИЯ ОБ ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ**

## Наименование объекта: информационная система персональных данных «ТИПОВАЯ ТИРАЖНАЯ СИСТЕМА ЭЛЕКТРОННЫЙ АРХИВ ООО «ИНТЕР РАО-ИТ» (Далее - ИСПДн);

## Расположение объекта: г. Москва, ул. Большая Пироговская, д. 27, Бизнес центр Луч.

## Класс защищенности объекта: в отношении ИСПДн определен 3 (третий) уровень защищенности;

## Перечень подсистем входящих в состав ИСПДн

В состав ИСПДн входят следующие системы/подсистемы:

1. Подсистема антивирусной защиты. Подсистема предназначена для обеспечения защиты от сетевых атак на АРМ и серверы ТТС ЭА на уровне узла (отслеживание и последующее блокирование во входящем сетевом трафике активности, характерной для сетевых атак), а также защиты от заражения вирусами файловой системы серверов и компьютеров. Подсистема представлена антивирусом Kaspersky Endpoint Security и Kaspersky Security для виртуальных сред. В состав подсистемы антивирусной защиты входят следующие функциональные модули:
   1. Модуль управления подсистемой антивирусной защиты.
   2. Модуль антивирусной защиты АРМ и серверов.
   3. Модуль антивирусной защиты среды виртуализации.
2. Подсистема межсетевого экранирования и обнаружения вторжений. Подсистема предназначена для организации многоуровневой защиты периметра сети ООО «Интер РАО - ИТ» и сегментов ТТС ЭА с осуществлением фильтрации трафика на основе заданных политик с возможностью обработки сетевого трафика до уровня приложений включительно (L7 относительно семиуровневой модели OSI). Подсистема представлена межсетевыми экранами FortiGate 3200D (кластер из двух нод), FortiGate 2500D (кластер из двух нод), двумя серверами управления FortiManager 2000E и двумя серверами централизованного сбора логов FortiAnalyzer 3000F. В состав подсистемы входят следующие функциональные модули:
   1. Модуль межсетевого экранирования и обнаружения вторжений уровня внешнего периметра сети.
   2. Модуль межсетевого экранирования и обнаружения вторжений пользовательских сегментов.
   3. Модуль межсетевого экранирования и обнаружения вторжений сервисного сегмента.
   4. Модуль межсетевого экранирования и обнаружения вторжений серверной группы ИСПДн
   5. Модуль управления.
   6. Модуль сбора событий.
3. Подсистема защиты среды виртуализации. Подсистема предназначена для разграничения доступа администраторов виртуальной инфраструктуры к гипервизорам (vCenter и ESX’i-серверам), а также обеспечения доверенной загрузки виртуальных машин. Подсистема представлена решением vGate R2.
4. Подсистема защиты от несанкционированного доступа. Подсистема предназначена для идентификации и аутентификации пользователей на АРМ и серверах ТТС ЭА, с последующим разграничением доступа к ресурсам файловой системы и программному обеспечению. Подсистема представлена СЗИ от НСД Secret Net Studio.
5. Подсистема криптографической защиты информации. Подсистема предназначена для обеспечения защиты персональных данных при передаче их по неконтролируемым каналам связи (Интернет и MPLS). Подсистема представлена криптошлюзами ViPNet Coordinator HW5000 4.x (два кластера по два криптошлюза), сервером централизованного управления ViPNet Administrator 4.x (КС3), сервером управления политиками безопасности ViPNet Policy Manager 4.x, сервером централизованного мониторинга ViPNet StateWatcher 4.x и программными клиентами ViPNet Client. В состав подсистемы входят следующие функциональные модули:
   1. Модуль криптографической защиты удаленного доступа.
   2. Модуль криптографической защиты доступа локальных пользователей.
   3. Модуль управления.
   4. Модуль централизованного управления политиками фильтрации трафика.
   5. Модуль централизованного мониторинга состояния сетевых узлов.
   6. Модуль персонального межсетевого экранирования.
6. Подсистема сбора и анализа событий безопасности. Подсистема предназначена для сбора и хранения событий безопасности с различных типов источников ТТС ЭА с последующим их анализом и обнаружением попыток несанкционированного доступа. Подсистема представлена решением MaxPatrol SIEM.
7. Подсистема анализа защищенности. Подсистема предназначена для обеспечения сканирования инфраструктуры ТТС ЭА (АРМ пользователей, сетевое оборудование, серверы) с целью выявления уязвимостей, связанных с ошибками в конфигурации общесистемного и прикладного программного обеспечения информационной системы, сетевого оборудования, а также программно-аппаратных средств защиты. Подсистема представлена решением MaxPatrol 8.
8. Подсистема защиты web-приложений, предназначенная для обеспечения доступности, целостности и конфиденциальности данных web-ресурсов ТТС ЭА.

## Количество АРМ пользователей и серверов

Автоматизированные рабочие места администраторов системы и разработчиков – 51 шт;

Типовое рабочее место пользователя – 150 шт;

Сервера – кластер из 6 серверов;

Виртуальные машины, на базе которых развернуты компоненты защищаемой системы ТТС ЭА – 13;

**Приложение №2**

к техническому заданию

**КАЛЬКУЛЯЦИЯ**

**трудозатрат на оказание услуг**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Исполнитель:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | |
| **Адрес:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | |
| **Заказчик:** |  |  |  |  |

1. Расчет трудозатрат

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Подсистема | | | | Детализация оказания услуг | Трудозатраты, чел/дни | Стоимость,  чел/дни | Итого стоимость чел/дни |
| 1 | 2 | | | | 3 | 4 | 5 | 6 |
| 1 |  | | | |  |  |  |  |
|  |  |  |
|  |  |  |
| 2 |  | | | |  |  |  |  |
|  |  |  |
|  |  |  |
| 3 |  | | | |  |  |  |  |
|  |  |  |
|  |  |  |
|  |  | | | |  |  |  |  |
|  |  | | | |  |  |  |  |
|  |  | | | |  |  |  |  |
|  | | | **Итого, из них:** | | | | |  |
| **1** | |  | |  | | | |  |
| **2** | |  | |  | | | |  |
| **3** | |  | |  | | | |  |
| **4** | |  | |  | | | |  |
| **5** | |  | |  | | | |  |
| **6** | |  | |  | | | |  |
| **…** | |  | |  | | | |  |

1. Под типовыми сегментами здесь и далее понимаются автоматизированные рабочие места, серверное оборудование, оборудование систем хранения данных, оборудование сетей передачи данных, взаимодействующие информационные системы. Сегмент считается соответствующим сегменту ОИ, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищенности, угрозы безопасности информации, реализованы одинаковые проектные решения по информационной системе и ее системе защиты информации. [↑](#footnote-ref-1)
2. Методика в т.ч. должна включать порядок действий работников Заказчика по оценке произведенных или планируемых изменений на предмет соответствия требованиям к типовым сегментам, а также порядок внесения корректировок в документацию при таких изменениях. [↑](#footnote-ref-2)