ПРИЛОЖЕНИЕ №1 К ДОКУМЕНТАЦИИ

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

на оказание услуг по проектированию системы безопасности значимых объектов КИИ

1. ОБЩИЕ СВЕДЕНИЯ
   1. Перечень сокращений:

|  |  |
| --- | --- |
|  | |
| Сокращение | Расшифровка сокращения |
| АРМ | Автоматизированное рабочее место |
| ИС | Информационная система |
| ИТКС | Информационно-телекоммуникационная сеть |
| АСУ | Автоматизированная система управления |
| КИИ | Критическая информационная инфраструктура |
| ЗОКИИ | Значимый объект критической информационной инфраструктуры |
| СБЗОКИИ | Система безопасности значимого объекта критической информационной инфраструктуры |
| ФСБ России | Федеральная служба безопасности Российской Федерации |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю Российской Федерации |
| РД | Руководящий документ |
| НСД | Несанкционированный доступ |

1. ОБЩИЕ ТРЕБОВАНИЯ К ОКАЗАНИЮ УСЛУГ
   1. В рамках оказания услуг по проектированию ЗОКИИ Исполнитель, при условии выполнения Заказчиком своих обязательств, должен разработать СБЗОКИИ в соответствии с приказом ФСТЭК   
      от 25 декабря 2017 года № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» со следующими этапами:

* Этап №1 «Обследование ЗОКИИ»;
* Этап №2 «Формирование требований к системе защиты ЗОКИИ»;
* Этап №3 «Разработка системы защиты ЗОКИИ».
  1. Оказание услуг осуществляется Исполнителем применительно к ЗОКИИ Заказчика, согласно таблице №1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | Таблица №1 | | |
| № | Адрес | Тип ЗОКИИ (ИС, АСУ, ИТКС) | | Наименование ЗОКИИ, количество | Программно-аппаратный состав |
| 1 | Калужская обл., г. Калуга, ул. Новаторская, д. 6  Калужская обл., г. Калуга, пер. Суворова, д. 8а | ИС | | ИСУЭЭ | Пользовательские компьютеры в составе: системный блок, монитор, мышь, клавиатура – 4 шт.,  Сервер – 4шт.,  Базовые станции (УСПД) – 260 шт.,  Счетчик электроэнергии – 67000 шт. |
| 2 | Калужская обл., г. Обнинск, ул. Студгородок, д. 1 | АСУ | | АСУ ТП ГТУ ТЭЦ | - Пользовательский компьютер в сборе (системный блок, процессор, материнская плата, вентилятор, монитор, клавиатура, мышь) – 6 шт.,  - Физический сервер управления – 1 шт.,  - Котел водогрейный № 1,  - Газовая горелка CIB UNIGAS – 1 шт.,  - Котел водогрейный № 2,  - Газовая горелка THERMINATOR – 1 шт.,  - Газотурбинная установка LM2500 DLE sn IMS-2008-LM208 – 1 шт.,  - Щит управления турбинной установкой САУ ГТУ – 1 шт.  - Шкаф автоматики и управления САРГОН – 3 шт.,  - Шкаф управления вентилятором горелки – 1 шт.,  - Шкаф управления дымососом – 1 шт.,  - Шкаф управления вентилятором дымососа – 1 шт.,  - Щит силовой – 1 шт.,  - Щит управления ПВК-1 – 1 шт.,  - Щит управления ПВК-2 – 1 шт.,  - Пульт управления ПВК-2 – 1 шт.,  - Щит силовой дымососа ДС-2 – 1 шт.,  - Система газовых трубопроводов подачи – 1 шт.,  - Система трубопроводов вентиляции – 1 шт.,  - Бак пермеата № 1 – 1 шт.,  - Бак пермеата № 2 – 1 шт.,  - Система трубопроводов очистки и подачи воды – 1 шт.,  - Бак деаэрированной воды БДВ № 1 – 1 шт.,  - Бак деаэрированной воды БДВ № 2 – 1 шт.,  - Система трубопроводов подачи воды – 1 шт.,  - Комплекс подготовки осмоса – 2 шт.,  - Система трубопроводов подачи осмоса – 1 шт.,  - Комплекс щитов управления – 10 шт.,  - Щит автоматики и управления УХЛ4, зав. № 3239 – 1 шт.,  - Шкаф центральной сигнализации ЩЭ-ЦС-1001 УХЛЗ, зав. № 325 в составе: блок управления, сириус ЦС, радиус автоматика, устройство резервной сигнализации – 1 шт.,  - Щит ПАС ИБ УХЛ4, зав. № 3065 – 1 шт.,  - Система трубопроводов котла утилизатора – 1 шт.,  - Дренажный трубопровод напорный клапанов котла утилизатора – 1 шт.,  - Котел утилизатор – 1 шт.,  - Система трубопроводов регулирования перепадов давления НЦКУ – 1 шт.,  - Резервуар водохранения – 2 шт.,  - Насосная система подпитки котла утилизатора – 1 шт.,  - Насосная система подачи и регулирования водоподачи – 1 шт.,  - Система трубопроводов фильтрации выбросов – 1 шт.,  - Щит управления вентилятором ЦС ДС-2,  - Система пожарной сигнализации – 1 шт., в составе:  1) Приемно-контрольный прибор С2000М,  2) Прибор контроля двухпроводной линии адресных извещателей С2000КДЛ,  3) Блок сигнализации С2000БКИ,  4) Датчики дыма, пламени, извещатели ручные ДИП 34А,  5) Модули управления светозвуковым оповещением,  - Система видеонаблюдения – 1 шт., в составе:  1) IP-камера HiWatch DS-1250L(B) – 19 шт.,  2) IP-камера HiWatch DS-1200(D) – 4 шт.,  3) Источник бесперебойного питания APC Easy UPS – 2 шт. |

* 1. Требования к гарантийным обязательствам.

На все результаты оказания услуг должны распространяться обязательства гарантийного сопровождения, предоставляемые Исполнителем, а также их доработку и устранение недостатков в случае необходимости.

* 1. Исполнитель должен обеспечить соблюдение правил действующего внутреннего трудового распорядка, контрольно-пропускного режима, внутренних положений и инструкций, действующих   
     на субъекте КИИ Заказчика.
  2. С целью надлежащего исполнения Исполнителем своих обязательств Заказчик обеспечивает:
     1. Доступ сотрудникам Исполнителя на объекты информатизации, входящие в программно-аппаратный состав ЗОКИИ, документам и сведениям, необходимым Исполнителю   
        для надлежащего оказания услуг.
     2. Предоставление Исполнителю информации и исходных данных в объеме достаточном   
        для разработки Исполнителем документации, являющейся результатом оказания услуг, а именно:
* данные для связи с должностным лицом со стороны Заказчика, ответственного   
  за взаимодействие с Исполнителем в рамках оказания услуг по настоящему Договору/Контракту: ФИО, мобильный телефон, электронная почта;
* сведения об ЗОКИИ (назначении, архитектуре объекта, применяемых программных средствах (системном, прикладном программном обеспечении и т.п.), информационных средствах (базах данных, файлах данных и т.п.), программно-аппаратных средствах (компьютерах, серверах, коммутационном оборудовании, носителях данных и т.п.), взаимодействии с другими ИС, ИТКС, АСУ, наличии и характеристиках доступа   
  к сетям связи);
* сведения о взаимодействии ИС, ИТКС, АСУ с другими ИС, ИТКС, АСУ и (или) о зависимости функционирования ИС, ИТКС, АСУ от других таких объектов;
* список предполагаемых пользователей для ЗОКИИ;
* информацию о режиме обработки информации в ЗОКИИ (многопользовательский   
  или однопользовательский);
* информацию о разграничение прав доступа пользователей для ЗОКИИ (с разграничением прав доступа или без разграничения прав доступа);
* информацию об уровне обобщения (обезличивания) персональных данных, в случае   
  их обработки;
* сведения об организации охраны и физической защиты помещений объекта информатизации.
  + 1. Система защиты проектируются с учетом, что АРМ, входящие в программно-аппаратный состав ЗОКИИ, отвечают следующим требованиям:
* АРМ/сервер должны в полном объеме соответствовать системным и иным требованиям, предъявляемым Производителями поставляемых СЗИ;
* АРМ/сервер должны функционировать под управлением операционных систем не ниже Windows 10 (32/64-разрядная), семейство Linux, а также отечественные операционные системы с актуальной версией ядра.
  1. Исполнитель вправе поэтапно/досрочно осуществить оказание услуг.
  2. Документы (Акт\\УПД), фиксирующие сдачу-приемку оказанных услуг, по согласованию сторон могут быть оформлены либо по факту сдачи-приемки соответствующей услуги, либо по результатам полного исполнения сторонами своих обязательств.
  3. В случае выявления противоречий в положениях Договора/Контракта и/или его приложениях, положения ТЗ имеют приоритетное значение.

1. ТРЕБОВАНИЯ К КАЧЕСТВЕННЫМ ХАРАКТЕРИСТИКАМ ОКАЗЫВАЕМЫХ УСЛУГ
   1. Этап №1 «Обследование ЗОКИИ»

В рамках Этапа №1 Исполнитель определяет актуальные угроз безопасности информации для ЗОКИИ.

Целью анализа угроз безопасности информации является определение возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учетом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов ЗОКИИ, взаимодействия с иными ОКИИ, информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями (далее – архитектура значимого объекта), а также особенностей функционирования значимого объекта.

Анализ угроз безопасности информации должен включать:

* выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
* анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств;
* определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;
* оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

В качестве исходных данных для анализа угроз безопасности информации Исполнителем должен использоваться банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России (<https://bdu.fstec.ru/>).

Модель угроз безопасности информации должна содержать краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя,   
и описание всех угроз безопасности информации, актуальных для значимого объекта.

Описание каждой угрозы безопасности информации должно включать:

* источник угрозы безопасности информации;
* уязвимости (ошибки), которые могут быть использованы для реализации (способствовать возникновению) угрозы безопасности информации;
* возможные способы (сценарии) реализации угрозы безопасности информации;
* возможные последствия от реализации (возникновения) угрозы безопасности информации.
  1. Этап №2 «Формирование требований к системе защиты ЗОКИИ»

В рамках Этапа №2 Исполнитель разрабатывает техническое задание (частное техническое задание)   
на создание СБЗОКИИ.

Техническое задание на создание системы защиты информации разрабатывается Исполнителем   
в соответствии с требованиями ГОСТ 34.602-2020. «Техническое задание на создание автоматизированной системы» и должно содержать организационные и технические требования к системе защиты информации ЗОКИИ, подлежащие реализации в рамках создания системы защиты информации ЗОКИИ.

Требования должны обладать следующими характеристиками: единичность, непротиворечивость, актуальность, выполнимость, проверяемость и однозначность.

Техническое задание должно включать:

* цель и задачи обеспечения безопасности значимого объекта или подсистемы безопасности значимого объекта;
* категорию значимости значимого объекта;
* перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект;
* перечень типов объектов защиты значимого объекта;
* требования к организационным и техническим мерам, применяемым для обеспечения безопасности значимого объекта;
* стадии (этапы работ) создания подсистемы безопасности значимого объекта;
* требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;
* требования к защите средств и систем, обеспечивающих функционирование значимого объекта (обеспечивающей инфраструктуре);
* требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями;

требования к составу и содержанию документации, разрабатываемой в ходе создания значимого объекта.

* 1. Этап №3 «Разработка системы защиты ЗОКИИ»
     1. Для достижения требуемого результата Исполнитель обеспечивает:
* разработку Технического проекта на создание системы защиты информации ЗОКИИ;
* разработку программ и методик испытаний;
* разработку плана реагирования на компьютерные инциденты;
* разработку комплекта организационно-распорядительной документации.
  + 1. При проектировании системы безопасности ЗОКИИ:
* определяются субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа;
* определяются политики управления доступом (дискреционная, мандатная, ролевая, комбинированная);
* определяются и обосновываются организационные и технические меры, подлежащие реализации в рамках системы безопасности ЗОКИИ;
* определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта;
* осуществляется выбор средств защиты информации и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;
* разрабатывается архитектура системы безопасности значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации;
* определяются требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта;
* определяются меры по обеспечению безопасности при взаимодействии значимого объекта   
  с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.
  + 1. Результатом разработки программ и методик испытаний является:
* «Программа и методики предварительных испытаний системы защиты ЗОКИИ»;
* «Программа опытной эксплуатации системы защиты ЗОКИИ»;
* «Программа и методики приемочных испытаний системы защиты ЗОКИИ»;
  + 1. Разработка плана реагирования на компьютерные инциденты.

Исполнитель осуществляет разработку плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак на информационные ресурсы, включая политику управления компьютерными инцидентами.

* + 1. Разработка комплекта организационно-распорядительной документации

Исполнитель осуществляет разработку внутренних приказов и другой внутренней организационно-распорядительной документации.

Комплектность, виды документов и обозначения технического проекта должны соответствовать ГОСТ.

3.4 По результатам выполненных работ Исполнитель разрабатывает следующий комплект документации:

* Модель угроз безопасности информации ЗОКИИ;
* Техническое задание на создание системы защиты ЗОКИИ;
* Технический проект на создание системы защиты ЗОКИИ;
* План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак на информационные ресурсы;
* Политика управления на компьютерные инциденты;
* Комплект шаблонов организационно-распорядительной документации.

1. ПОРЯДОК, УСЛОВИЯ И СРОКИ ОКАЗАНИЯ УСЛУГ

Исполнитель обязуется проводить работы по сбору исходных данных ЗОКИИ по адресу места нахождения Заказчика. Для этого специалист со стороны Исполнителя выполняет выезд по адресам места оказания услуг с целью обследования ЗОКИИ и сбора необходимой для оказания услуг информации.

Заказчик обязан в день и в месте прибытия Исполнителя, предоставить информацию в соответствии   
с п.2.5.2 настоящего Технического задания.

Сроки оказания услуг Заказчиком составляют 100 (сто) рабочих дней со дня вступления текущего Договора в силу.

1. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ
   1. Общие требования

Язык оформления документации – русский, за исключением общепринятых названий и оригинальных наименований программно-аппаратных средств импортного производства.

Документы должны быть оформлены Исполнителем в соответствии с требованиями оформленный   
в соответствии с требованиями ГОСТ Р 2.105–2019 «Общие требования к текстовым документам».

С целью надлежащего исполнения Сторонами своих обязательств, состав, объем, наименования, требования к содержанию документации могут быть скорректированы Сторонами в ходе оказания услуг.

* 1. Требования к документам, разрабатываемым в рамках настоящего ТЗ.

Комплект документации, разрабатываемой Исполнителем, оформляется в электронном виде в формате \*.docx. или \*.pdf. и направляется Заказчику в одном экземпляре, посредством отправки на электронную почту уполномоченного (ответственного) лица со стороны Заказчика: zhmykhov.ga@ksk.kaluga.ru.

Документы, подлежащие утверждению/согласованию Исполнителем, оформляются на бумажных носителях и утверждаются/согласовываются Заказчиком.

Комплект документации на бумажных носителях передается Заказчику нарочно или направляется заказным почтовым отправлением с уведомлением о вручении.

1. ТРЕБОВАНИЕ К БЕЗОПАСНОСТИ ОКАЗЫВАЕМЫХ УСЛУГ
   1. Все сведения о составе и характеристиках объектов информатизации Конечных пользователей   
      и Заказчика являются конфиденциальной информацией.
   2. Исполнитель обязуется:

* не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся на объектах информатизации Заказчика;
* не осуществлять несанкционированный доступ к информационным ресурсам объектов информатизации Заказчика;
* не проводить незаконное копирование информации, циркулирующей или хранящейся   
  на объектах информатизации Заказчика;
* не предпринимать манипулирование информацией, циркулирующей или хранящейся   
  на объектах информатизации (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);
* не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;
* не внедрять на объектах информатизации программы-вирусы (загрузочные, файловые и др.);
* не устанавливать программные и аппаратные закладные устройства в технические средства объектов информатизации Заказчика;
* не устанавливать в технические средства объектов информатизации программное обеспечение, зараженное вирусами.
  1. Нарушение настоящих требований влечёт за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законом Российской Федерации.

1. ТРЕБОВАНИЯ СООТВЕТСТВИЯ НОРМАТИВНЫМ ДОКУМЕНТАМ
   1. Услуги должны быть оказаны в соответствии с требованиями следующих нормативных   
      и правовых актов Российской Федерации в области обеспечения информационной безопасности:

* Федеральный закон от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях   
  и о защите информации»;
* Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
* постановление Правительства РФ от 8 февраля 2018 г. N 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации   
  и их значений»;
* приказ ФСТЭК России от 22 декабря 2017 г. N 236 «Об утверждении формы направления сведений   
  о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;
* Федеральный закон от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности»;
* постановление Правительства Российской Федерации от 16.04.2012 № 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 03.02.2012 N 79 "О лицензировании деятельности по технической защите конфиденциальной информации";
* приказ ФСТЭК России от 21 декабря 2017 г. N 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
* приказ ФСТЭК России от 25 декабря 2017 г. N 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
* МД ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Указ Президента РФ от 30 марта 2022 г. N 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации";
* Постановление Правительства РФ от 22 августа 2022 г. № 1478 (ПП № 1478) о требованиях к программным продуктам критической информационной инфраструктуры, применяемым в государственных организациях;
* Постановление Правительства PФ от 14 ноября 2023 г. № 1912 (ПП № 1912,) утверждающее порядок перехода субъектов КИИ на отечественные разработки;
* Приказ Минцифры от 18 января 2023 г. № 21, которым утверждены Методические рекомендации о порядке внедрения российского ПО для критической информационной инфраструктуры;
* Приказ Минпромторга от 6 марта 2023 г. № 722, утверждающий отраслевой план мероприятий для изменения стратегии закупок ПО для объектов критической информационной инфраструктуры у компаний из России;
* ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
* ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;
* ГОСТ 34.601-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;
* ГОСТ 34.602-2020 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы;
* ГОСТ 34.603-92 Информационная технология (ИТ). Виды испытаний автоматизированных систем;
* ГОСТ 34.201-2020 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.
  1. Исполнитель должен соответствовать требованиям, установленным в соответствии с статьей 12 Федерального закона от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности» к лицам, осуществляющим оказание услуг, являющихся объектом закупки, а именно:
* наличие собственной действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, при условии наличия в данной действующей лицензии работ (услуг), предусмотренных подпунктами «б», «в», «д», «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого постановлением Правительства Российской Федерации от 03 февраля 2012 г. № 79.