Техническое задание

|  |  |  |
| --- | --- | --- |
| № пп | Требование | Информация |
|  | Заказчик | ООО «Технология» |
|  | Наименование объекта (проекта) | Раздел: Информационная безопасность |
|  | Ориентировочное время начала работ, Сроки исполнения работ | Начало: 02.03.2020г.  Окончание: 29.05.2020г. |
|  | Вид строительства (новое, реконструкция, техперевооружение) | Техперевооружение |
|  | Натуральные показатели объекта | Реконструкция ПС 110 кВ. |
|  | Стадийность выполняемых проектных работ (ПД, РД) | РД |
|  | Разрабатываемые разделы | ИБ |
|  | Наличие экспертизы (ГОС, НЕГОС) | Не требуется |
|  | Технические требования к выполняемым работам | Объекты электроэнергетики.  Проектируется ВОЛС. В рамках проекта предусматривается установка системы мониторинга релейной защиты и автоматики (РЗА). Проектируемая сеть связи состоит из следующих узлов: 4 узла связи на которых устанавливается новое оборудование или доукомплектовывается существующее. Все узлы связи не обеспечены межсетевыми экранами, а также на них никогда не проводились мероприятия по повышению информационной безопасности. Из них: 1 узел связи - оборудование связи на данный момент отсутствует. 2 узел связи - оборудование существующее, планируется доукомплектация новым мультиплексором, необходимо предусмотреть межсетевой экран. 3 узел связи существующий, необходимо предусмотреть межсетевой экран. 4 узел связи существующий, выполняется доукомплектация мультиплексора.  Необходимо выполнить подключение к существующей технологической сети компании с системой информационной безопасности.  Разработать отдельный раздел рабочей документации «Подсистема информационной безопасности», в котором предусмотреть монтажные и пуско-наладочные работы проектируемой подсистемы ИБ.   1. В разделе «Подсистема информационной безопасности» предусмотреть реализацию, в том числе следующих технических мер по защите информации:    * 1. Межсетевое экранирование сегментов сети подстанции с применением межсетевых экранов с «горячим» резервированием;      2. Создание защищённых каналов связи с удалёнными АРМами.      3. Антивирусную защиту серверов и технологических АРМов с применением программного обеспечения Kaspersky Industrial Cybersecurtiy for Nodes;      4. Обеспечение передачи информации о выявленных инцидентах и угрозах ИБ в реальном времени в централизованную систему на базе программного обеспечения MaxPatrol SIEM.      5. Разработать описание архитектуры подсистемы безопасности проектируемой системы;      6. Разработать схему основного и резервного питания СЗИ;      7. Разработать схемы организации VPN-туннелей;      8. Разработать план IP-адресации;      9. Разработать схемы взаимодействия компонентов проектируемой подсистемы ИБ с сетевой инфраструктурой ОАО «Сетевая компания» (системами мониторинга, регистрации событий ИБ, SCADA системами, АСУ РЗА и ПА, системами резервного копирования и т.п.) с указанием протоколов взаимодействия, моделей активного сетевого оборудования, форматов передачи данных, адресации сегментов ЛВС и СПД, VPN туннелей;      10. Разработать матрицу информационных потоков, циркулирующих как внутри подсистемы ИБ проектируемого РАС, так и входящих, и выходящих за пределы этой подсистемы: 2. наименование проектируемой подстанции; 3. назначение ИП; 4. тип ИП (основной/резервный); 5. IP адрес источника информации; направление ИП; 6. интерфейс/скорость передачи (кбит/с); 7. сигнализация/протокол; 8. программные порты назначения/протокол; 9. IP адрес приёмника информации; 10. наименование VLAN; 11. диапазон IP-адресов VLAN; 12. оборудование, на котором терминирован VLAN (тип, месторасположение).     * 1. Разработать схему(ы) информационных потоков между пользователями, администратором РАС и непосредственно циркулирующих в РАС.       2. Разработать логические схемы с учётом сегментации локальной вычислительной сети (ЛВС) и сети передачи данных (СПД) с IP-адресацией, через которые организуется взаимодействие РАС с внешними информационными системами и взаимодействие составных частей РАС между собой.       3. Выполнить перечень сведений о проектируемых технологических серверах и АРМах (при наличии) данные с которых подлежат резервному копированию с указанием: 13. сетевого имени; 14. типа сервера (физический, виртуальный), АРМа; 15. типа и версии ОС; 16. роли сервера (АРМа); 17. объекта резервного копирования (образ системы целиком, конфигурационные файлы, БД и т.д.); 18. типа и версии используемой СУБД/приложений; 19. места расположения объектов резервного копирования на файловой системе сервера (АРМа); 20. требуется ли BMR (Bare Metal Restore) для клиента; периодичности резервного копирования; 21. временного окна резервного копирования; 22. адреса (наименования площадки) расположения сервера (АРМа); 23. объёма данных подлежащих резервному копированию.     * 1. Определить 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 РАС, АРМ, а также систем МП УРЗА;       2. Разработать порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации;       3. Разработать правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации);       4. Разработать схемы размещения СЗИ в телекоммуникационном(ых) шкафу(ах) на проектируемых площадках;       5. Разработать спецификацию оборудования и программного обеспечения;       6. Разработать программу и методику предварительных испытаний;       7. Разработать программу опытной эксплуатации;       8. Разработать программу и методику приёмочных испытаний.       9. Разрабатываемые организационные и технические меры по обеспечению безопасности не должны оказывать негативного влияния на создание и функционирование защищаемых информационных систем и информационно-телекоммуникационного оборудования.       10. При создании подсистемы ИБ необходимо максимально использовать возможности существующего оборудования в том числе и на смежных площадках проектирования.       11. При определении требований к параметрам настройки подсистем резервного копирования технологических серверов и АРМов (при наличии) рассмотреть в качестве места хранения данных систему резервного копирования, размещённую в управлении филиала или управления СК.       12. Для обеспечения технических мер по защите информации защищаемых систем должны применяться сертифицированные ФСТЭК России СЗИ или средства, прошедшие оценку соответствия в форме испытаний или приёмки в соответствии с Федеральным законом от 27.12.2002 №184-ФЗ «О техническом регулировании».       13. Проектная организация должна обладать лицензией Федеральной Службы по техническому и экспортному контролю России на деятельность по технической защите конфиденциальной информации, включающей в себя следующие виды работ и услуг: проектирование в защищённом исполнении: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений. 24. Разрабатываемые организационные и технические меры по обеспечению информационной безопасности не должны оказывать негативного влияния на создание и функционирование защищаемых информационных систем и информационно-телекоммуникационного оборудования. 25. При создании подсистемы ИБ необходимо максимально использовать возможности существующего оборудования в том числе и на смежных площадках проектирования. 26. Для обеспечения технических мер по защите информации защищаемых систем должны применяться сертифицированные ФСТЭК России СЗИ или средства, прошедшие оценку соответствия в форме испытаний или приёмки в соответствии с Федеральным законом от 27.12.2002 №184-ФЗ «О техническом регулировании». 27. Проектная организация должна обладать лицензией Федеральной Службы по техническому и экспортному контролю России на деятельность по технической защите конфиденциальной информации, включающей в себя следующие виды работ и услуг: проектирование в защищённом исполнении: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений. 28. Проектируемые технические и организационные решения по информационной безопасности необходимо предварительно согласовать с Заказчиком. 29. Проект разработать с учетом требований методических указаний по ЭМС (РД 34.20.116.-93.СО34.35.311-2004 и др. трасса кабельных лотков, дополнительные заземленные провода вдоль лотков, заземление, экранирование и др.). 30. Организация системы коммерческого учета электроэнергии:     1. Предусмотреть организацию системы коммерческого учета электроэнергии в КРУН 10кВ, присоединений ОРУ 110кВ на ПС 110 кВ, с применением электронных счетчиков активной и реактивной энергии класса точности 0.2S с подключением по 4-х проводной схеме.     2. Подключение расчетных счетчиков электроэнергии на  ПС 110 кВ произвести к существующей системе АИИСКУЭ.     3. Определить перечень исполнительной документации, с отражением в соответствующих листах проектной (рабочей) документации, детализированный по видам работ.     4. Принципиальные технические решения по проектированию и выбору оборудования до начала детальной разработки согласовать с Заказчиком;     5. Проектную документацию выполнить в 4-х экземплярах на бумажном носителе и один экземпляр проекта представить в электронном виде (на CD в формате AutoCAD и PDF) заказчику (НкЭС), сметную документацию в формате совместимости с ПК «Гранд-смета». |
|  | Бюджет | 250 000 руб. без НДС - для ООО/АО.  Стоимость работ в объявлении указана в базисе цен для юридических лиц.  При указании стоимости просьба указать стоимость в базисе цен согласно выбранному способу сотрудничества. |
|  | Условия оплаты (этапность оплаты: наличие аванса и т.д.) | Расчет – безналичный.  Аванс – не более 20%.  80% - оплата по итогам согласования результатов работ |
|  | Исходные данные | Все необходимые исходные данные будут предоставлены исполнителю перед началом работ. Дополнительные исходные данные предоставляются по запросу |

В заявке просим указать:

1) Планируемую форму сотрудничества (ООО/АО/ИП)

2) Опыт выполнения аналогичных работ

Предоставление дополнительной информации возможно по запросу.

Необходимые исходные данные Исполнителю будут предоставлены перед началом работ.