Шаблон технического задания для размещения проекта на ПИРС

|  |  |  |
| --- | --- | --- |
| № пп | Требование | Информация |
|  | Заказчик | ООО «Технология» |
|  | Наименование объекта (проекта) | Раздел Информационная безопасность |
|  | Ориентировочное время начала работ, Сроки исполнения работ | Начало: 30.12.2019г. Сроки: 25 календарных дней. |
|  | Вид строительства (новое, реконструкция, техперевооружение) | Техперевооружение |
|  | Натуральные показатели объекта ( | Замена существующего регистратора аварийных событий (РАС) на современный на ПС 110 кВ Поисево. |
|  | Стадийность выполняемых проектных работ (ПД, РД) | ПД, РД |
|  | Разрабатываемые разделы | ИБ |
|  | Наличие экспертизы (ГОС, НЕГОС) | Не требуется |
|  | Технические требования к выполняемым работам | Разработать отдельный раздел рабочей документации «Подсистема информационной безопасности», в котором предусмотреть монтажные и пуско-наладочные работы проектируемой подсистемы ИБ.  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: * наименование проектируемой подстанции; * назначение ИП; * тип ИП (основной/резервный); * IP адрес источника информации; направление ИП; * интерфейс/скорость передачи (кбит/с); * сигнализация/протокол; * программные порты назначения/протокол; * IP адрес приёмника информации; * наименование VLAN; * диапазон IP-адресов VLAN; * 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: * сетевого имени; * типа сервера (физический, виртуальный), АРМа; * типа и версии ОС; * роли сервера (АРМа); * объекта резервного копирования (образ системы целиком, конфигурационные файлы, БД и т.д.); * типа и версии используемой СУБД/приложений; * места расположения объектов резервного копирования на файловой системе сервера (АРМа); * требуется ли BMR (Bare Metal Restore) для клиента; периодичности резервного копирования; * временного окна резервного копирования; * адреса (наименования площадки) расположения сервера (АРМа); * 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. |
|  | Бюджет | 100 000 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 10%.  Поэтапная оплата по итогам передачи на проверку промежуточных 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.