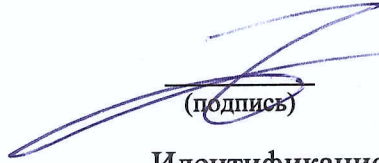


УТВЕРЖДАЮ

Директор ВЭС филиала
ПАО «Россети
Московский регион»
Гутнев Ф.С.


(подпись)

Идентификационный номер специалиста

		-						
--	--	---	--	--	--	--	--	--

« _____ » _____ 2025 г.

**Задание на проектирование
по титулу: «Модернизация ПС 110 кВ Фрязино с установкой комплексов
регистрации аварийных процессов»**

ПРОЕКТНАЯ ОРГАНИЗАЦИЯ

(наименование организации)

(должность)

(Ф.И.О.)

(подпись)

« _____ » _____ 2025 г.
М.П.

ГИП _____
(Ф.И.О.) (подпись)

Идентификационный номер специалиста

--	--	--	--	--	--	--	--	--	--

Москва 2025 г.

1. Основание для проектирования

1.1. Инвестиционная программа ПАО «Россети Московский регион».

1.2. Программа внедрения и модернизации регистраторов аварийных событий (РАС) на подстанциях ПАО «Россети Московский регион» на 2022-2027 гг. утвержденная первым заместителем генерального директора – главным инженером ПАО «Россети Московский регион» Д.Б. Гвоздевым и согласованная с филиалом АО «СО ЕЭС» Московским РДУ.

1.3. Регламент подготовки, согласования и утверждения ТУ, ЗП и ПСД на сооружение, техническое перевооружение и реконструкцию объектов ПАО «Россети Московский регион» (далее – регламент) в действующей редакции.

2. Нормативно-технические документы, определяющие требования к оформлению и содержанию проектной документации.

НТД указаны в приложении 1 к типовому заданию на проектирование ПАО «Россети». Также необходимо учесть следующие НТД:

- Постановление Правительства РФ от 18 ноября 2006 г. №697 «О внесении изменений в Классификацию основных средств, включаемых в амортизационные группы». Раздел 3 Техника электронно-вычислительная.

- Приказ ОАО «МОЭСК» от 09.09.2013 №931р «О снижении аварийности и подъеме уровня эксплуатации РЗиА в ОАО «МОЭСК».

- Распоряжение ОАО «МОЭСК» от 13.08.2014 №495 «Об организации эксплуатации комплексов регистрации аварийных процессов на объектах ОАО «МОЭСК».

При проектировании необходимо руководствоваться последними редакциями документов, необходимых и действующих на момент разработки документации.

3. Заказчик

«Восточные электрические сети» – филиал ПАО «Россети Московский регион».

4. Проектная организация (генеральный проектировщик)

Определяется по итогам конкурса (торгово-закупочных процедур по выбору подрядной организации на выполнение ПИР).

5. Сроки начала и окончания проектирования

Начало - с момента заключения договора на выполнение ПИР.

Окончание – сроки окончания договора ПИР.

6. Вид строительства и этапы разработки проектной документации.

6.1. Вид строительства: реконструкция.

6.2. Этапы разработки документации:

- ПД - разработка, согласование проектной документации (ПД) в соответствии с требованиями нормативно-технических документов; обеспечение подрядчиком получения заключения о достоверности определения сметной стоимости объекта.

- РД - разработка и согласование рабочей документации (РД) в соответствии с требованиями нормативно-технических документов.

6.3. ПД согласовывается с собственниками объектов, технологически связанных с объектом проектирования, в объеме технических решений, выполняемых на соответствующих объектах.

Основные технико - экономические показатели

Принять по утверждённым прогрессивным технико-экономическим показателям,

нормам и аналогам. Предусмотреть мероприятия по снижению материалов и энергоёмкости, трудовых и финансовых затрат.

Проектно-сметная документация должна быть разделена на мероприятия, учтенные и не учтенные укрупненными нормативами цен.

Объем финансовых потребностей мероприятий, учтенных укрупненными нормативами цен, необходимых для выполнения работ по строительству (реконструкции) в сводно-сметном расчете, не должен превышать объема финансовых потребностей для данных мероприятий, рассчитанных в соответствии с Приказом Министерства энергетики Российской Федерации от 17 января 2019г. №10 «Об утверждении укрупненных нормативов цены типовых технологических решений капитального строительства объектов электроэнергетики в части объектов электросетевого хозяйства».

7. Основные характеристики проектируемого объекта.

7.1. В части ПС 110 кВ Фрязино

Наименование мероприятия	Технологические решения
Номинальные напряжения (высший класс напряжения), кВ	110 кВ
Реконструкция и технологические решения	Выполнить работы по модернизации подстанции с установкой комплексов регистрации аварийных процессов
Общие требования к оборудованию ПС	1. Применяемое оборудование должно быть аттестовано в ПАО «Россети», соответствовать требованиям технической политики ПАО «Россети», Приказа ПАО «Россети» от 29.03.2019 г. №64 «Об утверждении стандартов организации», Распоряжения ПАО «Россети» от 19.03.2018 г. №106р «Об утверждении технических требований к компонентам цифровой сети» и Методических указаний ПАО «Россети Московский регион», Российским стандартам и быть сертифицированными в установленном порядке.
Релейная защита и автоматика (РЗА)	1. Проектирование релейной защиты и автоматики и последующие строительно-монтажные и пусконаладочные работы по РЗА выполнить в соответствии с результатами предпроектного обследования объекта с учётом следующих нормативно-технических документов: – Распоряжение ПАО «МОЭСК» от 20.03.2014г. №203 «О типовых функциональных схемах» – Распоряжение ПАО «МОЭСК» от 13.08.2014г. №495 «Об организации эксплуатации КРАП» – Распоряжение ОАО «МОЭСК» № 385р от 09.06.2014 года «Об утверждении требований к оформлению схем размещения защит». – Приказ Минэнерго России от 13.02.2019 №100 «Об утверждении Правил взаимодействия субъектов электроэнергетики, потребителей электрической энергии при подготовке, выдаче и выполнении заданий

Наименование мероприятия	Технологические решения
	по настройке устройств релейной защиты и автоматики». – Приказ Минэнерго России от 13.02.2019 № 101 «Об утверждении требований к оснащению линий электропередачи и оборудования объектов электроэнергетики классом напряжения 110 кВ и выше устройствами и комплексами релейной защиты и автоматики, а также к принципам функционирования устройств и комплексов релейной защиты и автоматики». – Приказ Минэнерго России от 10.07.2020 № 546 «Об утверждении требований к релейной защите и автоматике различных видов и ее функционированию в составе энергосистемы и о внесении изменений в приказы Минэнерго России от 8 февраля 2019 г. № 80, от 13 февраля 2019 г. № 100, от 13 февраля 2019 г. № 101». 2. Выбор типа вновь устанавливаемых устройств при проведении модернизации устройств защиты и автоматики определить проектом в соответствии с требованиями технической политики ПАО «Россети Московский регион» и «Рекомендаций по модернизации, реконструкции и замене длительно эксплуатирующихся устройств релейной защиты и автоматики энергосистем» (СТО 34.01-4.1-011-2020). 3. Проект должен содержать расчет и выбор параметров срабатывания пусковых органов КРАП. 4. Устройства КРАП выполнить на базе микропроцессорных устройств. 5. Микропроцессорные устройства РЗА, устанавливаемые на объекте проектирования, объектах, технологически связанных с объектом проектирования, и объектах, на которых предусматривается выполнение работ, должны обеспечивать свою работу при частоте 45,0 - 55,0 Гц. 6. В составе проекта по РЗА предусмотреть следующее: 6.1. Общие данные (назначение, цель). 6.2. Технологические решения (структура, электропитание оборудования комплексов регистрации аварийных процессов) по оборудованию. 6.3. Дополнительные технические решения (размещение на объектах, электропитание и инженерное обеспечение, определение мероприятий по обеспечению ЭМС МП устройств). 6.4. Организация строительства и эксплуатации (этапность и планирование, организация работ, организация эксплуатации). 6.5. Оценка основных технико-экономических показателей. 6.6. Схемно-технические решения по структуре КРАП. 6.7. Схемно-технические решения по размещению оборудования,

Наименование мероприятия	Технологические решения
	спецификаций оборудования и материалов, сметный расчет оборудования и материалов. 6.8. Технические решения по интеграции устанавливаемых устройств РЗА в существующие объектовые автоматизированные системы управления технологическим процессом, системы сбора и передачи информации. 6.9. В составе рабочей документации необходимо предоставить: - формы бланков в редактируемом формате (Word или Excel) - методики расчёта и выбора параметров настройки (уставок) и алгоритмов функционирования устройств - руководство по эксплуатации устройств РЗА, содержащее функционально-логические схемы и схемы программируемой логики с описанием алгоритма работы данных схем. 7. В целях обеспечения непрерывного контроля технологического процесса по передаче и распределению электроэнергии, фиксации хронологии событий, параметров электрических характеристик при технологических нарушениях для анализа работы комплекса устройств РЗА при установке КРАП, необходимо предусмотреть регистрацию сигналов в соответствии с требованиями Распоряжения ПАО «МОЭСК» от 13.08.2014г. №495 «Об организации эксплуатации КРАП». Представленный перечень сигналов не окончателен и может быть расширен при проведении предпроектного обследования. 8. Частота дискретизации данных при записи файлов осциллограмм должна выбираться из стандартного ряда частот, определяемых форматом Comtrade. Минимальная частота должна быть не менее 1000 Гц. 9. Пуск функции осциллографирования аварийных процессов должен осуществляться при наступлении одного из следующих условий: – выход аналоговым сигналом за границу верхней или нижней уставки; – изменение состояния дискретного сигнала на входе устройства; – выход расчетных значений токов и напряжений прямой, обратной и нулевой последовательности за границу верхней и нижней уставки. 10. Комплектное программное обеспечение должно предоставлять возможность: - производить анализ как осциллограмм, записанных средствами регистраторов, входящими в систему РАС, так и осциллограмм в формате Comtrade (IEC 60255-24 Edition 2.0), получаемых из сторонних источников;

Наименование мероприятия	Технологические решения
	- выполнения математических операций (например, сложение/вычитание, умножение, в том числе с применением комплексных коэффициентов) над измеренными и расчетными аналоговыми сигналами (с возможностью их индивидуального масштабирования и выполнения математических операций над ними, например, для формирования «фиктивного» сигнала вместо отсутствующего измерения одного из присоединений) с представлением их в виде расчетных аналоговых сигналов; - «наложения» выбранных пользователем аналоговых или дискретных сигналов (с представлением их в виде отдельного канала в осциллограмме и возможностью редактирования свойств их отображения, например, выделением каждого из сигналов различными цветами); - вычисления и отображения на осциллограмме симметричных составляющих аналоговых сигналов (прямая, обратная и нулевая последовательности); - построения векторных диаграмм токов и напряжений (фазных, линейных, составляющих прямой, обратной и нулевой последовательностей); - спектрального анализа (преобразования Фурье); - автоматического построения годографов сопротивлений (из фазных или линейных токов и напряжений, а также из расчетных аналоговых сигналов по заданию пользователя); - расчета частоты в выбранном канале (в том числе в расчетном) с возможностью отображения ее на осциллограмме; - расчета активной, реактивной, полной мощностей; - отображения на осциллограмме меток времени, интервалов времени, замеров значений векторов аналоговых сигналов (включая расчетные аналоговые сигналы). 11. Программное обеспечение должно функционировать на компьютерах под управлением операционной системы Microsoft Windows версий 2003 и выше. Все программное обеспечение должно быть русифицировано. 12. Оборудование регистрации аварийных процессов, устанавливаемое в рамках данного инвестиционного проекта, должно отвечать следующим техническим требованиям: - КРАП должен обеспечить регистрацию, хранение осциллограмм (в формате comtrade версии не ниже IEC 60255-24:2013) и журнала событий; - КРАП должен быть выполнен на базе микропроцессорных контроллеров, с естественным охлаждением основных элементов (без вентиляторов); - КРАП должен иметь открытый протокол обмена между измерительными преобразователями и сервером; - КРАП должен поддерживать стандартные протоколы обмена данными с внешними системами и терминалами РЗА: МЭК 61850-8.1 (MMS/GOOSE), МЭК60870-5-101, МЭК60870-5-103, МЭК60870-5-

Наименование мероприятия	Технологические решения
	104, МЭК60870-6-TASE.2; - КРАП должен иметь функцию автоматической записи с сервера на usb- накопитель файлов аварийных записей и исполнительной документации по проекту с контролем события вставки usb-накопителя в сервер; - КРАП должен иметь возможность интеграции в систему АСУТП (при ее наличии), а также возможность подключения к МП терминалам РЗА, установленным на ПС, и сбора информации о состоянии устройства и работе функций. - при возникновении условий для пуска функции осциллографирования аварийных процессов регистратор должен осуществлять непрерывную запись значений всех аналоговых сигналов, а также данных по изменению всех дискретных сигналов. Соответствующие файлы с записями аварийных событий должны храниться в памяти устройства и передаваться на верхний уровень АСУ ТП. Передача осциллограмм на верхний уровень должна осуществляться и во время записи осциллограммы. - поддержка протоколов обмена данными по шине процесса с МУ/регистраторами и интеллектуальными устройствами (коммутационные аппараты, измерительные трансформаторы) МЭК61850-9.2 (SV); - общее время записи файлов аварийных событий должно складываться из трех частей: время регистрации предаварийного режима (время до возникновения условий для пуска регистратора), время фиксации аварийной режима и время регистрации послеаварийного режима. Длительность записи доаварийного режима должно составлять от 0,1 секунд до 5 секунд, длительность записи аварийного режима должно составлять от 0,1 секунд до 50 секунд, и длительность записи послеаварийного режима должно составлять от 0,1 до 50 секунд. - объем внутренней энергонезависимой памяти регистратора должен составлять не менее 256 Мбайт, должна быть обеспечена возможность переноса аварийных файлов на внешний носитель информации. Количество хранимых в памяти регистратора осциллограмм должно ограничиваться только свободной памятью устройства. - в составе документации завода-изготовителя КРАП должны быть рекомендации по эксплуатации, выполнению технического обслуживания и ремонта, расчету и выбору параметров срабатывания регистратора; - поддержка интерфейсов связи физического уровня Ethernet и RS-485. - КРАП должен иметь распределенную архитектуру конструктивного построения. - микропроцессорные регистраторы аварийных событий должны обладать собственными встроенными часами реального времени. Должна быть обеспечена возможность синхронизации времени встроенных часов от внешних источников точного времени.

Наименование мероприятия	Технологические решения
	Регламент технического обслуживания устанавливаемого КРАП должен предусматривать техническое обслуживание по фактическому состоянию, после приемки из наладки. Программное обеспечение сервера КРАП и программы для просмотра осциллограмм должны иметь возможность отображения и обработки осциллограмм следующих форматов: comtrade (все форматы); *.bb; *.brs; *.dfr; *.do; *.os*; *.aura; *.sg2; *.cfg; *.dat; *.hdr; reg***.***; *.rio; *.reh. 13. Серверы КРАП, устанавливаемые в рамках данной целевой программы должны быть подключены к централизованной системе контроля и регистрации аварийных процессов ПАО «Россети Московский регион» по каналам связи со скоростью не менее 64 кБит/с. 14. Срок службы РАС, а также каждой единицы оборудования в ее составе должен составлять не менее 25 лет.
Информационная безопасность	Применяется в случае модернизации, реконструкции или создания системы АСУ ТП (ТМ), СДТУ, АСМД, дистанционного управления КА и оборудованием РЗА. Состав представляемых на рассмотрение материалов проектирования: - анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии); - категории значимости объекта информационной инфраструктуры; решения по организационным и техническим мерам обеспечения информационной безопасности объектов информационной инфраструктуры; - требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации; - требования к защите средств и систем, обеспечивающих функционирование объекта информационной инфраструктуры (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 предоставляемым материалам в части подсистемы Информационной безопасности: Руководящие указания по установке и настройке средств защиты информации, настройке программных и программно-аппаратных средств безопасности объектов информационной инфраструктуры; Руководящие указания по риск-ориентированному управлению объектами информационной инфраструктуры (ИТТ активами), организации в рамках процесса эксплуатации установки критических

Наименование мероприятия	Технологические решения
	обновлений программного обеспечения для объектов; Руководящие указания по конфигурации параметров программных и программно-аппаратных средств информационно-телекоммуникационной сети для обеспечения безопасности объектов информационной инфраструктуры, в том числе по обеспечению безопасного удаленного мониторинга объектов информационной инфраструктуры Цифровой сети, организации удаленного доступа в информационно-телекоммуникационную сеть субъекта электроэнергетики; Разработать и согласовать программу информирования и обучение персонала объекта информационной инфраструктуры; Представить расчет нормативной численности персонала, ответственного за планирование и контроль мероприятий по обеспечению безопасности объекта информационной инфраструктуры, управление (администрирование) подсистемой информационной безопасности, управление средствами защиты информации, управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования значимого объекта, мониторинг и анализ зарегистрированных событий в значимом объекте, связанных с обеспечением безопасности (далее - события безопасности), сопровождение функционирования подсистемы безопасности значимого объекта в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документах по безопасности значимого объекта; Представить решения по централизованному управлению подсистемой безопасности объектов информационной инфраструктуры (при необходимости); Разработать и согласовать план мероприятий по обеспечению безопасности объектов информационной инфраструктуры на случай возникновения нештатных (непредвиденных) ситуаций; Разработать и согласовать проект Акта категорирования объекта критической информационной инфраструктуры. Материалы проектной и рабочей документации в части информационной безопасности согласовать с подразделением информационной безопасности Предприятия электрических сетей, Департаментом комплексной безопасности персонала, объектов и информационной безопасности ПАО «Россети Московский регион», а также иными заинтересованными лицами. Требования по обеспечению информационной безопасности. Порядок создания подсистемы информационной безопасности, построение этапов работ, а также разработка технической и рабочей документации должны соответствовать ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Наименование мероприятия	Технологические решения
	Обеспечить создание подсистемы информационной безопасности, а также обеспечить выполнение: требований 187-ФЗ от 26.07.2017г. «О безопасности критической информационной инфраструктуры Российской Федерации» и подзаконных актов; требований Приказа ФСТЭК от 14 марта 2014 г. № 31 - не ниже 3 класса защищенности автоматизированной системы управления; требований РД «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации» не ниже уровня 1 Г; требований Распоряжения ПАО «Россети» от 01.04.2016 № 140 «Об утверждении минимальных требований к информационной безопасности АСТУ» (в редакции распоряжения ПАО «Россети» от 27.04.2016 № 178р и распоряжения ПАО «Россети» от 08.02.2019 г. № 70р); средства защиты информации должны соответствовать требованиям не ниже 6-го или более высокого уровня доверия («Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденные приказом ФСТЭК России от 02.06.2020 N 76); Применяемое оборудование должно быть включено в Реестр промышленной продукции, произведенной на территории Российской Федерации. Применяемое программное обеспечение должно быть включено в Единый реестр российских программ для электронно-вычислительных машин и баз данных. Применяемое оборудование и программное обеспечение средств информационной безопасности, сети передачи данных, АСУТП, ТМ должно быть сертифицированным ФСТЭК России и/или допущенным к применению на объектах ПАО "Россети", в соответствии с требованиями Приказа ПАО «Россети» от 28.07.2020 № 329 «Об утверждении методики и порядка проведения проверки качества (аттестации) оборудования и типового регламента работы комиссии по допуску оборудования» и прошедшим проверку в соответствии с требованиями приказа ПАО «Россети» от 28.08.2020 № 391 «Об утверждении Методики проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических

Наименование мероприятия	Технологические решения
	средств защиты информации в электросетевом комплексе». В случае организации дистанционного управления оборудованием, обеспечить выполнение требований Приказа Минэнерго России от 26.12.2023 № 1215 "Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике. В случае модернизации, реконструкции или создания автоматизированной системы мониторинга и диагностики энергетического оборудования, обеспечить выполнение требований Приказа Министерства энергетики РФ от 06.11.2018 №1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования». При проектировании и выполнении работ, учесть мероприятия, выполняемые в рамках смежных проектов. Тома проектной и рабочей документации в части информационной безопасности и тома в части защищаемых объектов информационной инфраструктуры (системы АСУ ТП, ТМ, СДТУ, АСМД, дистанционного управления КА и/или оборудования РЗА) согласовать со структурным подразделением информационной безопасности филиала и ДИБ ИА Общества, а также Московским РДУ. Обеспечить комплексную защиту информации, определяющей режим функционирования и/или раскрывающей систему защиты конкретного объекта, в случае ее передачи за пределы контролируемой территории. 1) Оборудование структурных компонентов (функциональных систем и подсистем) систем обеспечения безопасности объекта, а также помещений, в которых размещаются центральный и локальные пульты управления с устанавливаемым в них оборудованием, должно проводиться с учетом реализации технических мероприятий по защите информации. 2) На структурные компоненты (функциональные системы и подсистемы) систем обеспечения безопасности объекта, разработать

Наименование мероприятия	Технологические решения
	модели угроз для каждого типа энергообъекта. 3) Обеспечить целостность информации при передаче по внешним каналам связи по протоколу МЭК 670-5-101/104 с использованием шифрования или технологии инспекции промышленных протоколов. 4) Обеспечить целостность информации при передаче по внешним каналам связи по протоколу МЭК 670-5-101/104 с использованием шифрования. 5) Требования информационной безопасности, применяемые на всех объектах защиты: в случае наличия парольной защиты доступа, все пароли по умолчанию должны быть изменены; парольная политика к объектам защиты должна соответствовать установленным требованиям: по сложности пароля (не менее 12 символов, обязательно наличие символов в разном регистре и наличие специальных символов), сроку действия паролей и истории паролей; доступ персонала вне зависимости от объекта защиты должен быть персонализирован, необходимо исключить (при наличии технической возможности) возможность доступа к объектам защиты под одной учетной записью (одним паролем) для различных работников; встроенные учетные записи на всех компонентах объектов защиты должны быть отключены; высший приоритет применения на объектах защиты должны иметь механизмы доступа с применением многофакторной аутентификации; незадействованный функционал и компоненты объектов защиты должны быть отключены; на всех объектах защиты и их компонентах, должны быть включены и настроены функции регистрации событий безопасности с передачей на специально выделенный сервер сбора информации подсистемы мониторинга информационной безопасности; по всем компонентам объектов защиты должны быть установлены процедуры обновлений безопасности, время применения обновления безопасности на компонентах объектов защиты не должно превышать 24 часов. 6) Требования информационной безопасности, применяемые

Наименование мероприятия	Технологические решения
	к информационно-телекоммуникационной сети (далее - ИТС): должен быть организован периметр технологического сегмента ИТС Объекта. Организация сетевого периметра ИТС Объекта должна быть обеспечена посредством межсетевых экранов; физическое соединение технологического сегмента ИТС Объекта с остальной ИТС Объекта при ее наличии, должно обеспечиваться только через устройство, реализующее функции межсетевого экранирования; физическое соединение технологического сегмента ИТС Объекта с остальной ИТС Объекта при ее наличии, должно обеспечиваться только через устройство, реализующее функции межсетевого экранирования; выделение сегментов должно обеспечиваться посредством, одновременного применения следующих технологий и методов в порядке эффективности защиты (при наличии такой возможности): физическое выделение, посредством организации сегментов за счет выделенных коммутирующих устройств, подключаемых только к межсетевым экранам (наиболее защищенный вариант); с применением средств криптографической защиты доступа к сети и защиты трафика (VPN) при условии, что указанные средства в сегменте образуются посредством установки специализированного ПО на каждом из конечных узлов (серверов, АРМ); VLAN; VRF. На каждом из Объектов в ИТС должны быть выделены сегменты управления: сегмент управления ИТС (имеет доступ персонал, осуществляющий функции управления ИТС); сегмент управления АСТУ (имеет доступ персонал, осуществляющий функции управления АСТУ); сегмент управления подсистемами ИБ; сегмент оперативного управления Объектом (имеет доступ персонал, осуществляющий оперативное управление оборудованием Объекта). доступ к технологическому сегменту ИТС и другим входящим в него сегментам АС должен осуществляться только из сегмента оперативного управления. взаимодействие сегментов должно ограничиваться следующими правилами: доступ к сегментам управления из других сегментов запрещен; взаимодействие между сегментами должно происходить исключительно через средства межсетевого экранирования; взаимодействие между сегментами автоматизированных систем должно обеспечиваться в случае необходимости только посредством выделения специализированных выделенных «буферных» сегментов; правила на межсетевых экранах должны быть максимально точными включая указание адресов назначения и источника, портов

Наименование мероприятия	Технологические решения
	назначения и источника. для взаимодействия с внешними сетями и АС должны создаваться «демилитаризованные» зоны – сегменты сети, в которые могут обращаться внешние «потребители» и из которых исключена возможность инициации соединений во внутренние сегменты сети Объекта; служебные протоколы оборудования образующего ИТС, должны быть доступны только из сегмента управления ИТС; должны быть отключены неиспользуемые и небезопасные (передающие информацию по сети в открытом, незашифрованном виде) протоколы и сервисы на сетевом оборудовании; неиспользуемые порты на коммутационном оборудовании должны быть отключены логически и физически; доступ на уровне ИТС должен осуществляться в случае необходимости дополнительных мер с применением протоколов 802.1x и фильтрации MAC адресов; устройства беспроводной связи должны находиться физически и логически за организованным периметром ИТС Объекта; технологические протоколы необходимо строго изолировать от внешнего проникновения; на сетевом оборудовании должны быть включены функции от подмены сетевых адресов и меры защиты от внедрения ложной маршрутной информации в протоколы маршрутизации; должен быть включен сбор событий на уровне трафика в сети и передаваться на сервер подсистемы мониторинга информационной безопасности для контроля легитимности сетевых соединений. 7) Требования информационной безопасности, применяемые к автоматизированным системам (далее АС): каждая АС должна быть изолирована, от других АС, при необходимости взаимодействия с другими АС, взаимодействие должно быть обеспечено методами исключающими возможность его использование в деструктивных целях для обоих АС; при необходимости сбора необходимой информации с АС, указанные АС должны позволять передавать информацию посредством отправки технологической и другой информации иницируя соединения самостоятельно (по примеру протокола Syslog). Методы в виде опроса сервисов, баз данных и т.д. систем должны быть исключены; должно обеспечиваться резервирование конфигураций и баз данных АС; все применяемые АС должны иметь актуальную и доступную проектную и эксплуатационную документацию; в целевом исполнении АС должны иметь механизмы электронной подписи и криптографической защиты информации, а также должны обладать процедурами двойного контроля или паритета ответственности, когда выполнение критических действий невозможно выполнить одновременно одним лицом; прямой доступ к базам данных АС должен быть исключен;

Наименование мероприятия	Технологические решения
	территориально распределенные АС, с выведенным функционалом по управлению на централизованное удаленное управление в частности АСТУ, должны позволять осуществлять перевод управления на нижний (местный, Объектовый уровень). Функция отключения указанного внешнего управления должна гарантировать исключение возможности включения удаленного управления из вне; при выполнении контроля за АС необходимо обеспечить контроль за всеми ее компонентами на каждом конкретном Объекте (уровень системного программного обеспечения, уровень прикладного программного обеспечения (далее - ПО), уровень баз данных). 8) Требования информационной безопасности, применяемые к автоматизированным рабочим местам (далее АРМ) и серверам: на серверах АС и АРМ в обязательном порядке должны быть установлены средства антивирусной защиты с актуальными обновлениями; должна быть исключена возможность использования внешних устройств беспроводной связи на серверах и АРМ (блокировка необходимых портов как физически, так и логически); подключение внешних устройств хранения данных по умолчанию должно быть запрещено, подключение должно быть вызвано потребностью технологического бизнес-процесса и только на ограниченное время с контролем со стороны работника службы безопасности; должны быть включены пароли на доступ к встроенному ПО (BIOS, UEFI, сервисы управления) серверов и АРМ; должен применяться только необходимый и согласованный состав ПО на АРМ и серверах. При наличии возможности со стороны средств безопасности, установленных на АРМ и серверах должна быть реализована политика белых списков в отношении, используемого ПО; в целом исполнении доступ к АРМ и серверам должен обеспечиваться посредством средств многофакторной аутентификации; подключение к сети Интернет АРМ, с которых осуществляется выполнение критических операций должно быть запрещено; должен производиться контроль за хранением на серверах и АРМ парольной информации. В случае выявления должны быть инициированы проверки целостности скомпрометированных узлов и незамедлительная замена парольной информации для всех учетных записей, а также ревизия учетных записей; на всех АРМ и серверах должны быть включены персональные межсетевые экраны с правилами минимально необходимыми для функционирования объектов защиты. Весь остальной сетевой доступ должен быть заблокирован. 9) Требования к оборудованию: на всем технологическом оборудовании Объекта и оборудовании

Наименование мероприятия	Технологические решения
	безопасности имеющим функции управления, должны быть максимально использованы функции безопасности при их наличии; оборудование должно подключаться только к своим сегментам ИТС; неиспользуемый функционал и интерфейсы связи должны быть отключены. 10) Требования к подсистемам информационной безопасности: Минимальный состав подсистем ИБ должен состоять из: - подсистемы антивирусной защиты; - подсистемы межсетевого экранирования ИТС и конечных узлов; - подсистемы анализа сетевого трафика и обнаружения компьютерных атак; - подсистемы мониторинга информационной безопасности (централизация сбора и анализа событий безопасности регистрируемых на конечных узлах Объекта с целью контроля и выявления нарушений). Предусмотреть сбор событий информационной безопасности для передачи в САЦ сетевой компании. Необходимость разработки мероприятий защиты информации для каждого конкретного объекта определяется по результатам предпроектного обследования. Использовать отдельные туннелированные каналы связи (стандарт VPN) для телеизмерений, учёта и качества электроэнергии, средств физической безопасности). Создаваемые в рамках проводимых работ центральные и удаленные пульта управления безопасностью должны быть аттестованы на предмет соответствия требованиям РД «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации» не ниже уровня 1Г. Требования к участникам: Участник торгово-закупочных процедур или член коллективного участника, чьими силами планируется выполнение работ в части обеспечения информационной безопасности, на момент подачи заявки должен отвечать следующим требованиям по наличию: Лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации согласно п.п. б), г), д), е) ст.4 Положения введенного Постановлением Правительства РФ 2012 года № 79; Лицензии ФСБ на осуществлении работ по пунктам 2, 3, 8, 9, 12-14, 21-23 «Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении

Наименование мероприятия	Технологические решения
	шифровальных (криптографических) средств». Нормативно-технические документы (НТД), определяющие требования к оформлению и содержанию проектной документации (ПД): Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»; Политика ПАО «Россети» в области информационных технологий, автоматизации и телекоммуникаций (Политика ИТТ, утверждена Советом директоров ПАО «Россети» (Протокол от 11.09.2017 №276); ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

8. Требования к оформлению и содержанию проектной документации.

Проектирование выполнить в соответствии с Постановлением Правительства РФ №87 от 16.02.2008г. (с изменениями и дополнениями) "О составе разделов проектной документации и требованиях к их содержанию" и в соответствии с ГОСТ Р 21.1101-2013 СПДС. Основные требования к проектной и рабочей документации.

До начала разработки проектной документации Проектировщик разрабатывает и согласовывает с Заказчиком состав проекта, в соответствии с которым осуществляется дальнейшее проектирование и приемка выполненных работ.

При проектировании необходимо руководствоваться последними редакциями документов, действующих на момент разработки проектно-сметной документации.

9. Особые условия.

Оформление текстовых и графических материалов, входящих в состав проектной документации, выполнить в соответствии с приказом Минрегиона России от 02.04.2009 № 108 «Об утверждении правил выполнения и оформления текстовых и графических материалов, входящих в состав проектной и рабочей документации».

Согласование документации осуществляется в системе «Архив ПСД» с заведением документации в электронном виде через личный кабинет Проектировщика.

Проектирование выполнить согласно требованиям Типового ЗП (распоряжение 628р от 17.11.2017).

При проектировании учитывать, в части касающейся, требования:

- «Методических указаний по применению в ПАО «Россети Московский регион» основных технических решений по эксплуатации, реконструкции и новому строительству электросетевых объектов», утвержденных приказом ПАО «Россети Московский регион» от 30.12.2019г. №1515.

10. Выделение этапов строительства, реконструкции.

Не требуется.

11. Исходные данные для разработки проектной документации.

Перечень исходных данных, сроки их подготовки и передачи определяются условиями Договора на разработку проектной документации и календарным графиком. Получение исходных данных проектной организацией выполняется с выездом на объекты. Заказчик обеспечивает организационную поддержку доступа представителей проектной организации для получения информации.

Исходные данные, передаваемые Заказчиком Проектной организации:

Настоящее ЗП.

Исходные данные предоставляются по письменному запросу от Проектной организации.

12. Прочие сведения.

12.1. Документация, передаваемая проектной организацией заказчику.

Сформировать и передать заказчику комплекты документации в полном объеме, в том числе:

Проектная и рабочая документация, согласованная в установленном порядке (комплект с согласованиями) передается заказчику в следующем количестве:

- бумажная версия – по 4 экземпляра;
- электронная версия в формате PDF (цвет, с согласованиями, с разбивкой по томам, каждый том отдельным файлом) – 3 экземпляра на 3-х компакт дисках (в т.ч. 2 экз. – для торгово-закупочных процедур);
- электронная версия в системе AutoCAD (*.dwg) и текстовые документы в системе MS Office – 1 экземпляр.

Сметная документация передается заказчику в следующем количестве:

- бумажная версия – 4 экземпляра;
- электронная версия в формате PDF – 3 экземпляра на 3-х компакт дисках (в т.ч. 2 экз. – для торгово-закупочных процедур);
- электронная редактируемая версия сметной документации:
- в формате Smeta.ru (*.sob) – 1 экз.;
- в формате АРПС 1.10. (*.apr) – 1 экз.;
- в формате MS Office Excel – 1 экз.

Количество экземпляров передаваемой проектной организацией заказчику по договору должно соответствовать указанному в ЗП.

12.2. Разработка программы ПНР и комплексного опробования (индивидуальных испытаний) оборудования.

При необходимости, разработать отдельным томом программу ПНР. Объем и нормы испытаний электрооборудования и ПНР определить проектом в соответствии с требованиями СНиП 3.05.06-85 «Электротехнические устройства», производителей оборудования, ПУЭ «Правила устройства электроустановок».

Выполнить сметный расчет согласно требованиям МДС 81-40.2006 (Указания по применению федеральных единичных расценок на пусконаладочные работы) и ТСН-2001.5.

12.3. Требования по обеспечению защиты сведений, составляющих государственную тайну.

При использовании документов, содержащих секретные сведения, необходимо при выполнении работ обеспечить соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну.

Обеспечить выполнение требований закона РФ от 21.07.1993 №5485-1 «О государственной тайне».

12.4. Техническое заключение по проектной документации.

После получения согласований по всем томам проектной документации, Проектная организация готовит проект Технического заключения по проектной документации и направляет его Заказчику в редактируемом формате Word для дальнейшего рассмотрения и утверждения подразделением-инициатором титула.

Техническое заключение готовится в описательной форме в виде общей пояснительной записки и должно содержать разделы:

- I. Введение.
- II. Краткое содержание проекта.
- III. Замечания и предложения.
- IV. Выводы.

12.5. Согласование проекта.

Согласование документации с филиалом ПАО «Россети Московский регион» - «Восточные электрические сети» и всеми другими заинтересованными организациями выполняет Проектная организация.

Срок действия настоящего ЗП составляет 5 лет.

Заместитель директора - главный инженер
ВЭС – филиала ПАО «Россети МР»

Начальник службы РЗА ВЭС – филиала ПАО
«Россети МР»

Д.А. Уксеков

А.Г. Дроздов