УТВЕРЖДАЮ:

И.о. генерального директора
- заместитель генерального
директора по операционной деятельности
АО «МЭК «Энергоэффективные технологии»



_____ Бухвалов А.С.

«10» ноября 2026 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Выполнение работ по проектированию системы обеспечения информационной безопасности в составе программно-технического комплекса "Автоматизированная система технологического управления" в импортозамещенном исполнении (ПТК АСТУ) в интересах филиала ПАО «Россети Северо-Запад» в Республике Коми

2026 год

1. Перечень применяемых сокращений.

В тексте настоящего Технического задания использованы сокращения, приведенные в таблице 1.

Таблица 1. Применяемые сокращения

Сокращение/термин	Расшифровка/определение
ДЗО	Дочерние и зависимые общества
ИБ	Информационная безопасность
КИИ	Критическая информационная инфраструктура
ЛЭП	Линия электропередачи
Объекты КИИ	Объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры
ОКИИ	Объект критической информационной инфраструктуры – ПТК АСТУ
ОРД	Организационно-распорядительные документы
ПАО	Публичное акционерное общество
ПД	Проектная документация
ПО	Производственное отделение
ПП РФ	Постановление Правительства Российской Федерации
Проектная документация	Комплект документов (текстовых и графических), который определяет архитектурные, функционально-технологические, конструктивные и инженерно-технические решения для строительства, реконструкции или капитального ремонта объекта.
ПС	Подстанция
ПТК	Программно-технический комплекс
ПТК АСТУ	Программно-технический комплекс «Автоматизированная система технологического управления» в импортозамещенном исполнении (ПТК АСТУ) в интересах филиала ПАО «Россети Северо-Запад» в Республике Коми
РП	Распределительный пункт
РЭС	Районные электрические сети
СБ	Система безопасности
СКЗИ	Средство(-а) криптографической защиты информации
ТЗ	Техническое задание на проектирование программно-технического комплекса «Автоматизированная система технологического управления» в импортозамещенном исполнении (ПТК АСТУ) в интересах филиала ПАО «Россети Северо-Запад» в Республике Коми
ТИ	Телеизмерение
ТП	Трансформаторная подстанция
ТС	Телесигнализация
ТУ	Телеуправление
ФЗ	Федеральный закон
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ЦУС	Центр управления сетью

2. Общие сведения

2.1. Наименование работ

Выполнение работ по проектированию системы обеспечения информационной безопасности в составе программно-технического комплекса "Автоматизированная система технологического управления" в импортозамещенном исполнении (ПТК АСТУ) в интересах филиала ПАО «Россети Северо-Запад» в Республике Коми.

2.2. Наименование Заказчика

Заказчик: АО «МЭК «Энергоэффективные технологии» в интересах филиала ПАО «Россети Северо-Запад» в Республике Коми.

Адрес: 603000, г. Нижний Новгород, ул. Пискунова, д. 29, помещение П34. Почтовый адрес: 603155, г. Нижний Новгород, а/я 31.

2.3. Место и сроки выполнения работ

Место выполнения работ: Россия, Республика Коми, 167000, г. Сыктывкар, ул. Интернациональная, д. 94 и дистанционно по месту нахождения Подрядчика.

Сроки выполнения работ:

- начало выполнения работ: с момента заключения договора;
- окончание выполнения работ: не позднее 60 (шестидесяти) календарных дней с момента заключения договора.

2.4. Содержание работ по проектированию системы обеспечения информационной безопасности и требования к работам.

Подрядчик в соответствии с настоящим ТЗ подготавливает Проектную документацию. Проектная документация состоит из результирующих документов, указанных в п.2.4.1 – п.2.4.3 настоящего Технического задания.

2.4.1. Разработка технических решений по обеспечению информационной безопасности объекта, в том числе:

2.4.1.1. Уточнение категории объектов КИИ в соответствии с требованиями Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. № 187 ФЗ;

2.4.1.2. Составление перечня критических процессов в ПТК АСТУ;

2.4.1.3. Определение актуальных угроз безопасности информации в ПТК АСТУ;

2.4.1.4. Разработка решения по защите информации и мероприятий по их выполнению с учетом требований руководящих документов регулирующих органов;

2.4.1.5. Определение организационных мероприятий, применяемых для обеспечения информационной безопасности КИИ Объекта;

2.4.1.6. Разработка решения по взаимодействию объекта КИИ с иными объектами КИИ, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

2.4.1.7. Результатом выполнения работ, предусмотренных п. 2.4.1. Договора, является предоставление Заказчику следующих документов (результирующих документов):

–проект Акта категорирования ОКИИ Общества;

–проект Сведений об ОКИИ Общества для направления во ФСТЭК России;

–Модель угроз безопасности информации (нарушителя);

–Частное техническое задание на создание СБ объекта КИИ.

2.4.2. Техническое проектирование СБ объекта КИИ согласно требованиям информационной безопасности, установленным действующим законодательством РФ и пунктом 3 настоящего ТЗ.

В результате выполнения технического проектирования СБ объекта КИИ Подрядчиком должны быть предоставлены Заказчику следующие документы (результирующие документы):

–Пояснительная записка к техническому проекту СБ ОКИИ;

–Схема размещения комплекса технических средств СБ ОКИИ;

–Схема структурная СБ ОКИИ;

–Схема функциональная СБ ОКИИ;

–Ведомость технического проекта СБ ОКИИ;

–Ведомость с техническим характеристиками покупных оборудования, изделий, материалов СБ ОКИИ.

2.4.3. Разработка организационно-распорядительных документов по обеспечению безопасности ОКИИ.

В результате выполнения данных работ Заказчику передаются следующие проекты документов (результирующие документы):

–План мероприятий по обеспечению безопасности ОКИИ;

–Регламент выявления инцидентов ИБ в ОКИИ и реагирования на них;

–Регламент информирования и обучения персонала ОКИИ (с приложением формы журнала проведения инструктажей по ИБ, формы журнала ознакомления с ОРД по ИБ ОКИИ);

–Инструкция о порядке учета, хранения, обращения и уничтожения машинных носителей информации (с приложением формы журнала учета машинных носителей информации, формы акта уничтожения конфиденциальной информации или носителей, содержащих конфиденциальную информацию);

–Регламент управления конфигурацией ОКИИ и управления (администрирования) СБ ОКИИ;

–Документ о назначении администратора информационной безопасности ОКИИ;

–Документ об определении лиц, ответственных за планирование и контроль мероприятий по обеспечению безопасности ОКИИ;

–Документ об определении лиц, которым разрешены действия по внесению изменений в конфигурацию ОКИИ и ответственных за управление (администрирование) СБ ОКИИ;

–Документ об определении лиц (подразделения), ответственных за обеспечение безопасности ОКИИ, в том числе за выявление компьютерных инцидентов и реагирование на них;

–Документ о создании комиссии по осуществлению внутреннего контроля состояния безопасности (уровня защищенности) ОКИИ;

–Положение о комиссии по осуществлению внутреннего контроля состояния безопасности (уровня защищенности) ОКИИ (включая контроль за обеспечением безопасности ОКИИ);

–Регламент анализа уязвимостей ОКИИ;

–Документ о возложении на заместителя руководителя органа (организации) полномочий по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

–Положение о заместителе руководителя органа (организации), ответственного за обеспечение информационной безопасности органа (организации);

–Документ о возложении функций по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, на подразделение;

–Положение о структурном подразделении органа (организации), обеспечивающем информационную безопасность органа (организации);

–Документ об утверждении перечня сведений конфиденциального характера, обрабатываемых в ОКИИ;

–Документ об утверждении перечня лиц, имеющих доступ к защищаемой информации;

–Инструкция по организации работы с СКЗИ (с приложением формы журнала учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, формы акта об установке и вводе в эксплуатацию СКЗИ, формы акта уничтожения криптографических ключей и ключевых документов, формы технического (аппаратного) журнала, анкеты для тестирования пользователей СКЗИ);

–Документ об утверждении перечня лиц, допущенных к работе с СКЗИ (пользователей СКЗИ);

–Правила доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;

–Документ об утверждении перечня лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

2.5. Требования к оформлению Проектной документации

2.5.1. Подрядчик оформляет Проектную документацию в соответствии с нормативными требованиями, в том числе в соответствии с требованиями Постановления Правительства Российской Федерации от 16.02.2008 № 87 «О составе разделов проектной документации и требованиях к их содержанию».

2.5.2. В Проектной документации не допускается указывать наименования изготовителей и/или марки (в том числе технические условия на изготовление) проектируемого оборудования, систем.

2.5.3. Проектную документацию в полном объеме (включая обосновывающие расчеты) необходимо представить Заказчику:

–в 2 (двух) экземплярах на бумажном носителе, из которых не менее 1 (одного) экземпляра в оригинале. Каждый том оригинала и копии ПД должен быть прошит, заверен печатью и подписью руководителя, страницы пронумерованы. Все экземпляры томов копий Проектной документации должны быть заверены печатью «Копия верна»;

–в электронном виде на флеш-накопителе или CD диске:

- в формате pdf с текстовой подложкой для документов с текстовым, графическим содержанием;
- в форматах doc, docx, xls и/или xlsx для документов с текстовым содержанием;
- vsd и/или vsdx для документов с графическим содержанием;
- xls, xlsx для сводки затрат, сводного сметного расчета стоимости строительства, объектных сметных расчетов (смет), сметных расчетов на отдельные виды затрат;
- xml для локальных сметных расчетов (смет) на всех этапах проектирования в том числе ее согласования;
- в формате электронного архив.

2.6. Требования к проектным решениям

2.6.1. Проектные решения, разрабатываемые в рамках данного ТЗ, должны в обязательном порядке предусматривать использование отечественного программного обеспечения и радиоэлектронной продукции, включенного в Единый реестр российских программ для электронных вычислительных машин и баз данных (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановление Правительства Российской Федерации от 16.11.2015 № 1236, и Реестр промышленной продукции в соответствии с требованиями постановления Правительства Российской Федерации от 17.07.2015 № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации»).

2.7. Особые условия проектирования

2.7.1. Оформление текстовых и графических материалов, входящих в состав Проектной документации, должны быть выполнены в соответствии с приказом Минрегиона России от 02.04.2009 № 108. В Проектной документации должны использоваться диспетчерские наименования объектов электросетевого хозяйства.

2.7.2. При направлении откорректированных материалов Проектной документации Подрядчиком должны быть приложены перечень направляемых томов (разделов) и обоснованные ответы на поступившие замечания (в табличном виде в формате «принимается/не принимается» с указанием скорректированных №№ разделов, страниц и т. д. или мотивировкой отказа).

2.7.3. Проектная документация должна включать описание функциональных возможностей проектируемого состава технологического программного обеспечения.

2.7.4. Разработанная в соответствии с настоящим Техническим заданием Подрядчиком документация является собственностью Заказчика, и передача ее третьим лицам без его согласия запрещается.

2.7.5. Технические решения Проектной документации должны основываться на применении оборудования, материалов и систем, включенных в Перечень оборудования, материалов и систем, допущенных к применению на объектах ПАО «Россети», в противном случае в проектной документации указать на необходимость обязательного прохождения процедуры Проверки качества для соответствующих видов оборудования, материалов и систем, предусмотренной Порядком проведения проверки качества (аттестации) оборудования, материалов и систем в электросетевом комплексе на электросетевых объектах филиалов/ДЗО ПАО «Россети», утвержденным приказом ПАО «Россети» от 28.07.2020 № 329.

2.8. Приёмка выполненных работ

2.8.1. Работы считаются выполненными надлежащим образом в соответствии с условиями Договора и ТЗ в случае подписания Сторонами акта сдачи-приемки Результатов выполненных работ и передачи прав/ УПД без замечаний.

2.8.2. При выявлении в Проектной документации замечаний (недостатков) Заказчик направляет Исполнителю реестр выявленных замечаний (недостатков).

2.8.3. Если требуется доработка Проектной документации, Подрядчик обязан в срок, установленный Заказчиком и составляющий не более 5 (пяти) рабочих дней, провести указанную доработку и направить доработанную Проектную документацию в соответствии с требованиями п.2.5.3 Договора Заказчику.

2.8.4. В случае получения Подрядчиком повторных и последующих замечаний со стороны Заказчика к доработанной Проектной документации Исполнитель обязан осуществить доработку Проектной документации в порядке, указанном в настоящем разделе.

2.8.5. Приемка выполненных работ завершается оформлением акта сдачи-приемки Результатов выполненных работ/ УПД.

2.8.6. Основными критериями оценки результатов при приемке выполненных работ является соответствие требованиям действующего законодательства РФ, настоящего ТЗ и Договора.

2.9. Исходные данные для разработки Проектной документации

2.9.1. Исходные данные по объекту проектирования системы обеспечения информационной безопасности в составе программно-технического комплекса "Автоматизированная система технологического управления" в импортозамещенном исполнении (ПТК АСТУ) в интересах филиала ПАО «Россети Северо-Запад» в Республике Коми, необходимые Подрядчику для выполнения работ по Договору, предоставляются Заказчиком.

2.10. Гарантийный срок на выполненные работы

2.10.1. Срок предоставления гарантий качества выполнения работ составляет не менее 12 (двенадцати) месяцев с даты подписания акта сдачи-приемки Результатов выполненных работ и передачи прав/ УПД.

2.10.2. В течение всего гарантийного срока Подрядчик несет ответственность за качество разработанной Проектной документации, в том числе принимает претензии по качеству и производит исправление результатов работ в случае их некачественного выполнения. Срок устранения замечаний, возникших в период гарантийного срока, – не более 5 (пяти) рабочих дней с момента получения письменной претензии Заказчика, если иной срок не согласован Сторонами.

3. Нормативные документы

3.1. Все работы по проектированию системы обеспечения информационной безопасности в составе программно-технического комплекса "Автоматизированная система технологического управления" в импортозамещенном исполнении (ПТК АСТУ) в интересах филиала ПАО «Россети Северо-Запад» в Республике Коми необходимо проводить в соответствии с требованиями следующих документов:

−Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

−Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

−Указ Президента Российской Федерации от 30 марта 2022 года № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»;

−Указ Президента Российской Федерации от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

−постановление Правительства Российской Федерации от 8 февраля 2018 года № 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»;

−постановление Правительства Российской Федерации от 14 ноября 2023 года № 1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации»;

–приказ ФСТЭК России от 21 декабря 2017 года № 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 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

–приказ ФСБ Российской Федерации от 25 декабря 2025 года № 547 «Об утверждении Порядка информирования ФСБ Российской Федерации о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"»;

–методический документ «Методика оценки угроз безопасности информации» (утвержден ФСТЭК России 5 февраля 2021 года);

–методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;

–ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;

–ГОСТ Р 51275-2006 «Защита информации. Объект автоматизации. Факторы, воздействующие на информацию. Общие положения»;

–ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

–ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

–ГОСТ 34.602-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

–ГОСТ Р 59793-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

–ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»;

–ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;

–ГОСТ Р ИСО/МЭК 27001–2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

4. Меры по предоставлению национального режима

Основание: Постановление Правительства Российской Федерации от 23.12.2024 № 1875 «О МЕРАХ ПО ПРЕДОСТАВЛЕНИЮ НАЦИОНАЛЬНОГО РЕЖИМА ПРИ ОСУЩЕСТВЛЕНИИ ЗАКУПОК ТОВАРОВ, РАБОТ, УСЛУГ ДЛЯ ОБЕСПЕЧЕНИЯ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ НУЖД, ЗАКУПОК ТОВАРОВ, РАБОТ, УСЛУГ ОТДЕЛЬНЫМИ ВИДАМИ ЮРИДИЧЕСКИХ ЛИЦ».

Предоставление национального режима в соответствии с ПП 1875 от 23.12.2024.	
ОКПД 2	Мера применения национального режима (запрет, ограничение, преимущество)
71.12.12.190	Не применяется