


УТВЕРЖДАЮ

Заместитель директора по производству –
главный инженер
ООО «ЕвроСибЭнерго – Гидрогенерация»

 Ю.В. Дворянский

« 03 » октября 2022 г.

ЗАДАНИЕ

на выполнение комплекса работ по модернизации
«Техническое перевооружение автоматизированной системы управления
гидроагрегатами (АСУГ 1-18ГА) Братской ГЭС»

1. Основания для проектирования

- 1.1. Протокол совещания рабочей группы Эн+ по проверке энергетических Объектов группы на защищенность от кибератак от 14.10.2019.
- 1.2. Протокол совещания у Заместителя Совета Безопасности Российской Федерации от 27 мая 2020 года по вопросу «О повышении защищенности объектов критической информационной инфраструктуры Российской Федерации электроэнергетического комплекса».
- 1.3. План технического перевооружения систем АСУТП на филиалах ООО «ЕвроСибЭнерго-Гидрогенерация».

2. Вид строительства

Модернизация.

3. Район и площадка строительства

Иркутская область, г. Братск, филиал ООО «ЕвроСибЭнерго-Гидрогенерация» «Братская ГЭС».

4. Назначение проведения работ

- 4.1. Реализация работ по техническому перевооружению АСУГ одиночных и укрупненных блоков служит для выполнения следующих задач:
 - выполнение требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации в части защитных мер, выполнение которых является обязательным для значимого объекта КИИ 3 категории значимости;
 - выполнение требований по импортозамещению применительно к электронным компонентам системы и используемому ПО;
 - техническое перевооружение существующей физически и морально устаревшей системы управления.
- 4.2. Функции, выполняемые автоматизированной системой одиночного блока (генератор – трансформатор):
 - автоматический пуск гидроагрегата на холостой ход;

- подготовка схемы синхронизации гидроагрегата для включения в сеть;
- управление нагрузкой гидроагрегата;
- работа агрегата в режиме синхронного компенсатора;
- останов гидроагрегата (плановый и аварийный по защитам);
- гидромеханические защиты агрегата;
- блокировка схемы управления разъединителями генератора;
- предупредительная и аварийная сигнализация;
- термоконтроль гидроагрегата;
- контроль электрических и технологических параметров;
- диспетчерский контроль и управление;
- регистратор электрических параметров агрегата;
- регистрация технологической дискретной информации о работе оборудования;
- обеспечение необходимого температурного режима в помещениях кабельных вводов;
- обмен данными по цифровым интерфейсам с существующими и планируемыми к модернизации автоматизированными системами: СВ, ПТК ЭГР, ПТК ССМД, ПТК ЦСМЗ, ПТК АРЗ, РЗ ГА.

Режимы работы оборудования:

- нормальный (ГА в работе) с действующей системой связи с верхним уровнем;
- нормальный (ГА в работе), но связь с верхним уровнем отсутствует;
- ГА в ремонте, связь с верхним уровнем отсутствует;
- ГА в наладке с одновременной проверкой защит, автоматики, возбуждения с действующей системой связи с верхним уровнем.

4.3. Функции, выполняемые автоматизированной системой укрупненного блока (два генератора – трансформатор):

- автоматический пуск гидроагрегатов на холостой ход;
- синхронизация гидроагрегатов блока при включении в сеть;
- управление нагрузкой гидроагрегатов;
- работа агрегатов в режиме синхронного компенсатора;
- останов гидроагрегатов (плановый и аварийный по защитам);
- гидромеханические защиты агрегатов;
- управление совместным возбуждением генераторов блока;
- блокировка схемы управления разъединителями генераторов;
- управление задвижками ТВС при пуске, останове и изменении режима работы ГА (задвижка №44);
- предупредительная и аварийная сигнализация;
- термоконтроль гидроагрегатов;
- контроль электрических и технологических параметров;
- диспетчерский контроль и управление;
- регистратор электрических параметров агрегатов.
- обмен данными по цифровым интерфейсам с существующими и планируемыми к модернизации автоматизированными системами: СВ, ПТК ЭГР, ПТК ССМД, ПТК ЦСМЗ, ПТК АРЗ, РЗ ГА.

Режимы работы оборудования:

- нормальная работа ГА в составе укрупненного блока (для ГА ст. № 1 – 8) – ГА в работе в составе УБ с действующей системой связи с верхним уровнем;
- Работа ГА в составе укрупненного блока (для ГА ст. № 1 – 8) – ГА в работе в составе УБ, но связь с верхним уровнем отсутствует;

- в ремонте один ГА блока, ГА – в режиме ремонт из состава укрупненного блока исключен (для ГА ст.№ 1 – 8) связь с верхним уровнем отсутствует;
- наладка одного ГА с одновременной проверкой защит, автоматики, возбуждения на этом ГА, ГА – в режиме наладка из состава укрупненного блока исключен (для ГА ст.№ 1 – 8) с действующей системой связи с верхним уровнем.

4.4. Функции, выполняемые подсистемой верхнего уровня АСУГ:

- архивирование принятой информации о контролируемых технологических параметрах;
- обработка принятой информации в реальном масштабе времени;
- отображение технологического процесса в виде мнемосхем, графиков, истории событий;
- прием команд оператора и передача их нижний уровень;
- регистрация событий, связанных с контролируемым технологическим процессом и действиями персонала, ответственного за эксплуатацию и обслуживание системы;
- формирование отчетных форм на основе архивной информации.

4.5. Функции, выполняемые подсистемой измерения уровней верхнего и нижнего бьефа:

- данная система входит в АСУГ. Измеренные значения уровней и напора передаются в АСУГ каждого генератора для обеспечения работы алгоритмов перевода агрегатов в режим синхронного компенсатора. Также эти данные используются в ЭГР ГА и ГРАРМ для оптимизации работы агрегата и станции в целом.

5. Объем проектной и рабочей документации

5.1. Разработка проектной и рабочей документации на техническое перевооружение по объекту «Техническое перевооружение автоматизированной системы управления гидроагрегатами (АСУГ 1-18ГА) Братской ГЭС» проводится для:

- разработки технических решений по техническому перевооружению существующего комплекса АСУГ, позволяющих реализовать существующие требования к информационной безопасности управляющих систем, задачи импортозамещения, измерения и фиксации дополнительных параметров, необходимых для полноценной работы системы предиктивной диагностики гидроагрегата.
- выбора оборудования и разработки схемы по техническому перевооружению существующих АСУГ, позволяющих реализовать в полном объеме функции к автоматизированной системе, перечисленные в п.4, а также принятые и согласованные в результате проведения предпроектного обследования и разработки Технического задания технические решения;
- согласование выявленного в результате предпроектного обследования дополнительного перечня точек измерения, необходимого для организации эффективной и безопасной работы АСУГ и смежных с ней систем (в том числе для обеспечения работы всех диагностических правил автоматизированной системы предиктивной диагностики ГА), выбор удовлетворяющих поставленной задаче мест установки и монтажа дополнительного оборудования и датчиков;
- разработки надежной и резервированной схемы верхнего уровня, обеспечивающей непрерывную диагностику работоспособности всего оборудования, входящего в модернизированную систему и архивацию всех входных и выходных сигналов, как существующих, так и добавленных в рамках планируемого технического перевооружения;

- разработка надежной и резервированной схемы бесперебойного питания АРМ ВУ АСУГ, а также шкафов серверов ВУ АСУГ.

5.2. Проектную и рабочую документацию разработать на основе принятых в проектной документации технических, технологических и иных решений с учетом особенностей объекта и требований ГОСТ, ЕСКД, ЕСПД, СНиП, ПУЭ и других нормативно руководящих документов, действующих на территории Российской Федерации в объеме полного комплекта (основной комплект, прилагаемые и ссылочные документы) в соответствии с ГОСТ Р 51583-2014, ГОСТ 34.601-90, ГОСТ 34.602-2020, ГОСТ 34.201-2020, ГОСТ Р 59795-2021, СТО 59012820.29.020.009-2016, а также документов, указанных в разделе 5.3 настоящего задания на проектирование.

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

- Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- ГОСТ Р 59853-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения;
- ГОСТ 34.201-2020 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»;
- ГОСТ 34.602-2020 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении»;
- Приказ ФСТЭК России от 21 декабря 2017 г. №235 «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказ ФСТЭК России от 25 декабря 2017 г. №239. «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСТЭК России от 14 марта 2014 г. №31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;
- СТП ЕСЭГГ.503.520-2021 от 02.08.2021 «Техническая политика по развитию и эксплуатации АСУТП»;
- СТП 907-011.202.115-2020 «Ценообразование в ремонтной, строительной деятельности, услуг производственного и непроизводственного (технического) характера» ООО «ЕвроСибЭнерго-Гидрогенерация».

Данный список НТД не является полным и окончательным. При проектировании необходимо руководствоваться актуализированными редакциями документов, действующих на момент разработки проектно-сметной документации.

5.4. Проектная документация, разработанная в соответствии с действующими в РФ нормами, во всех её частях, в объеме достаточном для осуществления внедрения, скомпонованная в отдельных томах:

- Отчет о предпроектном обследовании с подробным описанием существующей системы имеющихся организационных и технических мер с приложением физических и логических схем по формату приложения (предпроектное обследование);
- Модель угроз (предпроектное обследование);
- техническое задание на создание автоматизированной системы управления ГА БГЭС. В техническом задании должны быть детализированы и согласованы все технические решения, необходимые для технического перевооружения АСУГ одиночного и укрупненного блока, сетевого оборудования и оборудования верхнего уровня, системы измерения верхнего и нижнего бьефа. Также, на этапе разработки и согласования технического задания должны быть детализированы и учтены все необходимые требования по информационной безопасности к данной системе, выделен раздел информационная безопасность;
- «Общая пояснительная записка». Том должен содержать всю описательную, расчётную и графическую часть, выполняемую в рамках осуществления внедрения;
- сметная документация;
- принципиально-монтажные схемы на модернизируемое и вновь устанавливаемое оборудование с привязкой к действующим устройствам и оборудованию;
- графические логические схемы и блок-схемы алгоритмов технологических процессов;
- монтажные схемы панелей, шкафов и оборудования;
- схемы кабельных связей;
- журналы кабельных связей (для демонтируемых и монтируемых кабелей);
- планы (чертежи) размещения оборудования и прокладки кабельных связей;
- сборочные и габаритные чертежи;
- спецификации оборудования, материалов, комплектующих и ЗИП.

Проектная документация на АСУГ для одиночного и укрупненного блока должна быть разработана как типовая, с возможностью ее использования при дальнейшей поэтапной реконструкции систем управления и сигнализации гидроагрегатов Братской ГЭС.

5.5. Рабочая документация должна включать в себя:

- ведомость документов;
- перечень входных сигналов (физических, цифровых; аналоговых, дискретных);
- перечень выходных сигналов (физических, цифровых; аналоговых, дискретных);
- спецификации оборудования, изделий и материалов;
- схема структурная комплекса технических средств;
- схема соединения внешних проводок;
- схема подключения внешних проводок;
- логические схемы локальной вычислительной сети АСУГ;
- физические схемы локальной вычислительной сети АСУГ;
- программы и методики испытаний компонентов, подсистем, систем, комплексов автоматизации;
- протоколы сетевых сервисов, отражающих информационный обмен между компонентами системы;
- протоколы сетевых сервисов, отражающих информационный обмен с внешними автоматизированными системами;
- параметры настроек компонентов системы для реализации механизмов информационной безопасности;
- комплект организационно-распорядительной документации по защите информации;

- план расположения оборудования и проводок;
- кабельный журнал;
- опросные листы для заказа оборудования;
- ведомости объемов работ;
- задание заводу на изготовление шкафов;
- пояснительная записка к техническому проекту;
- руководство администратора;
- руководство пользователя;
- руководство программиста;
- физическую и логическую схемы по формату приложения с подробной привязкой к объекту.

Комплект организационно-распорядительной документации по защите информации должен включать документы различного уровня (регламенты, положения, инструкции) и покрывать все требования по документированию процессов информационной безопасности, установленные приказами ФСТЭК России №235, №239 по обеспечению безопасности значимых объектов КИИ (По решению субъекта критической информационной инфраструктуры Требования приказа ФСТЭК России №239 могут применяться для обеспечения безопасности объектов критической информационной инфраструктуры, не отнесенных к значимым объектам. Если объект не является значимым объектом КИИ, к нему применяются требования как значимому объекту КИИ 3 категории значимости. Если объект является АСУТП, то в дополнение к требованиям приказа ФСТЭК России №239 должны быть выполнены требования приказа ФСТЭК России №31 в соответствии с установленным классом защищенности автоматизированной системы управления) и иными нормативными документами, в том числе комплект организационно-распорядительной документации должен определять правила и процедуры реализации отдельных организационных и (или) технических мер безопасности. Состав проектной документации может быть дополнен по предложению Исполнителя.

5.6. Рабочая документация разрабатывается на весь период технического перевооружения на основе утвержденных в проектной документации, технических и технологических решений в соответствии с действующими нормами, правилами и регламентами.

6. Основные данные и требования к проектным решениям

6.1. Предпроектное обследование:

- исполнитель должен провести обследование объекта с целью определения: расположения элементов модернизируемой системы, используемых портов, протоколов, используемого оборудования, ОС, ПО, нормативной документации, угроз безопасности, обеспечения их электропитанием, кабельных трасс, необходимости установки дополнительных датчиков и места их установки, необходимость переноса существующих и новые места их установки;
- предпроектное обследование проводится проектной организацией самостоятельно, с выездом специалистов на БГЭС. Заказчик обеспечивает доступ на объект и оказывает необходимое содействие в сборе исходных данных;
- результаты предпроектного обследования согласуются с Заказчиком, департаментом по эксплуатации "ЕвроСибЭнерго-Гидрогенерация", ДЗР Эн+ Менеджмент «Сибирь».
- По результатам предпроектного обследования в обязательном порядке должен быть подготовлен отчет с подробным описанием существующей системы с приложением физических и логических схем по формату Приложения и нормативной документации объекта

6.2. Модель угроз на целевую систему в соответствии с "Методическим документом. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021) (модель угроз разрабатывается в два этапа: предварительный до разработки ТЗ и окончательный после разработки проектной документации (уточнение модели угроз))

6.3. Разработка ТЗ

В составе документации разработать техническое задание на АСУТП согласно ГОСТ 34.602-2020 «Техническое задание на создание автоматизированной системы». В техническом задании учесть все требования по безопасности для проектируемого объекта на основании требований нормативных документов и принятой категории значимости (класса защищенности). В техническом задании выделить раздел по ИБ.

6.4. Разработка основных технических решений

- на основании данных, полученных при проведении предпроектного обследования необходимо определить перечень оборудования «Автоматизированной системы управления гидроагрегатами Братской ГЭС», модернизация и поставка которого требуется для выполнения работ и места его расстановки. Выполнить необходимый объем проектных работ;
- при проектировании необходимо выполнить требования Федеральной службы по техническому и экспортному контролю (ФСТЭК) по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (Проектные решения должны в полном объеме соответствовать требованиям приказов ФСТЭК №235 и №239 в части защитных мер (меры изложить подробно с привязкой к конкретному объекту и сопоставлением с разработанными на этапе проекта и уже существующими на объекте организационными и техническими мерами) , выполнение которых является обязательным для значимого объекта КИИ 3 категории значимости) По решению субъекта критической информационной инфраструктуры Требования приказа ФСТЭК России №239 могут применяться для обеспечения безопасности объектов критической информационной инфраструктуры, не отнесенных к значимым объектам. Если объект не является значимым объектом КИИ, к нему применяются требования как значимому объекту КИИ 3 категории значимости. Если объект является АСУТП, то в дополнение к требованиям приказа ФСТЭК России №239 должны быть выполнены требования приказа ФСТЭК России №31 в соответствии с установленным классом защищенности автоматизированной системы управления. В обязательном порядке в основные решения должны быть включены физические и логические схемы целевой системы.

6.5. Требования к техническому перевооружению АСУГ одиночного блока.

6.5.1. Требования к системе в целом.

АСУГ одиночного блока должна:

- быть сертифицирована органами Госстандарта России;
- быть оснащена средствами самодиагностики всех составляющих;
- содержать в своем составе только серийно выпускаемые промышленные контроллеры и программное обеспечение, имеющие в соответствии с законодательством Российской Федерации статус «российское происхождение»;
- в шкафах должны быть предусмотрены меры для защиты входных сигналов от помех;

- в шкафах должны быть предусмотрены модули гальванической развязки дискретных и аналоговых входных и выходных сигналов (гальваническая развязка входов/выходов диагностических сигналов в пределах шкафа не требуется);
- все источники питания должны иметь электронную защиту от перегрузки и токов короткого замыкания;
- ориентировочное количество физических входных-выходных сигналов должно составлять:
- дискретных входных сигналов – 400;
- дискретных выходных сигналов – 100;
- аналоговых входных сигналов – 200;
- должен быть предусмотрен 10% резерв по каналам управления и контроля.

6.5.2. Перечень подсистем, входящих в АСУГ одиночного блока:

Функционально следует выделить следующие подсистемы:

- подсистема приема и первичной обработки информации;
- подсистема управления гидроагрегатом;
- подсистема управления режимом синхронного компенсатора;
- подсистема контроля трансформатора;
- подсистема термоконтроля;
- подсистема диагностики;
- подсистема сигнализации;
- подсистема визуального представления и архивирования информации (операторская панель);
- подсистема обмена информацией с существующими и планируемыми к модернизации внешними автоматизированными системами: (СВ, ПТК ЭГР, ПТК ССМД, ПТК ЦСМЗ, ПТК АРЗ, РЗ ГА система мониторинга трансформатора (опционально)).

6.5.3. Требования к конструктивному исполнению:

АСУГ должна включать в себя:

- шкафы типа RITTAL с одной операторской панелью, либо аналогичные по конструктиву и качеству, стандартных габаритов 2200x800x600 двустороннего обслуживания с цоколем высотой 200 мм над уровнем пола;
- степень защиты шкафа, не ниже IP54;
- шкафы должны быть оборудованы лампами освещения, системой климат-контроля, контролем доступа;
- доступ к установленному в шкафах оборудованию должен осуществляться через переднюю и заднюю двери, оснащенные замками под ключ «четырёхгранник» 8 мм. Задние двери необходимо выполнить двухстворчатыми. На дверях предусмотреть размещение знака «Осторожно! Электрическое напряжение» со стороны треугольника 50 мм;
- связи с внешними устройствами должны осуществляться через клеммные ряды, расположенные с задней стороны шкафа. Требование к зажимам - подключение не более двух проводов к одному зажиму под винт. Сечение зажимаемых проводников от 0,2 до 2,5 мм².
- для подвода кабелей в днище шкафов должно быть предусмотрено достаточное количество кабельных вводов. Выше вводов должны располагаться зажимы для крепления кабелей;
- наличие шинок заземления внутри шкафов;
- внутри шкафов должны размещаться розетки 220В с выводом на клеммник шкафа для подключения аппаратуры во время наладки и проведения регламентных работ;

- на шкафах на лицевой и обратной стороне необходимо разместить надписи (таблички с надписью), соответствующие номеру шкафа и его наименованию;
- цвет окраски шкафов RAL 7035.

6.5.4. Требования по стандартизации и унификации:

При стандартизации должны учитываться особые требования к системе АСУГ:

- базовые конструкции ПТК - стойки, каркасы, навесные шкафы и т.п., должны выполняться в соответствии со стандартами ГОСТ 28601.2-90, ГОСТ 28601.3-90;
- выходы всех применяемых датчиков должны быть унифицированы и соответствовать требованиям ГОСТ 26.010-80, ГОСТ 26.011-80, ГОСТ 26.013-81.

При унификации должны учитываться особые требования к системе АСУГ:

- в ПТК должно использоваться минимальное количество питающих напряжений;
- номенклатура используемых конструктивных единиц должна быть сведена к минимуму. Конструктивы шкафов, рам, функциональных модулей должны быть унифицированы со всеми системами АСУ ТП БГЭС. Отдельные конструктивы шкафов (внешние размеры, цвет шкафа и цоколя, сторона крепления петель передних дверей, место размещения и размеры знаков безопасности, табличек с надписями, шрифты надписей) должны быть унифицированы с конструктивами шкафов, составляющих ряд АЦУ (БЦУ) в который будет устанавливаться шкаф АСУГ;
- формы представления информации оператору должны быть приближены к проектным изображениям технологических схем и их элементов;
- в ПТК должны применяться программируемые логические контроллеры одной фирмы;
- в УСО вне зависимости от типа используемых входных и выходных сигналов должен использоваться унифицированный интерфейс;
- программно-технические средства системы АСУГ должны быть серийно выпускаемыми. Не допускается применение морально устаревших технических средств, уникальных устройств и оборудования производителей, неизвестных в отрасли.

6.5.5. Требования к функциям системы:

- должны использоваться унифицированные контроллеры серийного производства со сроком службы не менее 10 лет. Должна быть обеспечена возможность замены в процессе эксплуатации однотипных элементов и устройств ПТК;
- АСУГ должна обеспечить управление гидроагрегатом, как в автоматическом, так и в ручном режиме работы;
- АСУГ должна управляться от двух резервированных контроллеров, каждый из которых содержит полный набор функций, необходимый для управления агрегатом. Контроллеры и модули контроллеров должны иметь исполнение, предусматривающие возможность горячей замены без отключения ГА от сети;
- устройства АСУГ должны являться самодостаточной частью АСУ ТП. При исчезновении связи с верхним уровнем система управления генератором должна продолжать функционировать в режиме местного управления.

Для обеспечения работы агрегатов в автономном режиме при отсутствии связи с верхним уровнем предусмотреть:

- сохранение физических (по кабельным жилам) сигналов управления с ЦПУ – сигналы управления регулятором скорости (всего 2 шт.);
- сохранение существующих обобщенных сигналов срабатывания сигнализации устройств РЗА (вторичных устройств) генератора на ЦПУ и существующее рабочее место НСЦ МЗ;
- в АСУГ необходимо предусмотреть резервирование гидромеханических защит и управления агрегатом;

- должна быть обеспечена возможность контроля и управления гидроагрегатом с рабочего места машиниста, расположенного в непосредственной близости от управляемого гидроагрегата.

6.6. Требования к техническому перевооружению АСУГ укрупненного блока:

Требования к техническому перевооружению АСУГ укрупненного блока в целом соответствуют требованиям к техническому перевооружению АСУГ одиночного блока с учетом наличия дополнительного оборудования, дополнительных режимов и блочного щита управления.

6.7. Требования к техническому перевооружению сетевого оборудования и оборудования верхнего уровня:

- должна быть реализована новая цифровая сеть с топологией «двойная звезда», дублированная как по линиям связи, так и по коммуникационному оборудованию, с контролем состояния сетевого оборудования;
- в состав системы сбора и архивации информации должны входить дублированные сервера ввода/вывода и дублированные сервера баз данных. Дублирование должно осуществляться посредством размещения основных и резервных серверов в разные шкафы – основные сервера ВВ и БД должны быть размещены в помещении ВЦУ (шкафы серверов 1), дублирующие сервера ВВ и БД должны быть размещены в помещении АСУ ТП (шкафы серверов 2);
- данные на серверах ВВ и БД должны быть защищены от несанкционированного доступа, в том числе от удаления или изменения. Серверы должны иметь возможность автоматического определения неработоспособности основного сервера и передачи всех функций дублирующему, а также возможность автоматической синхронизации данных в случае временной неработоспособности одного из серверов, для поддержания одинакового набора данных;
- сервера ВВ и БД должны быть дублированными, дублирующие сервера должны работать в горячем резерве;
- сервера ВВ и БД должны быть реализованы на базе серийно выпускаемой серверной платформы, и обеспечивать отказоустойчивость за счет дублированного блока питания с возможностью питания как переменным, так и постоянным током, с возможностью «горячей» замены и дублированных жестких дисков также с возможностью «горячей» замены;
- отказы блоков питания и жестких дисков серверов ВВ и БД, попытки несанкционированного доступа к серверам, признаки неработоспособности серверов должны сопровождаться сообщениями оперативному персоналу и фиксироваться в базе данных;
- должно быть предусмотрено архивирование всех аналоговых и дискретных входных и выходных параметров, а также неисправностей всех элементов подсистем АСУГ;
- должна быть предусмотрена возможность копирования заданной части архива за заданный промежуток времени на внешние носители для ее длительного хранения;
- в составе АСУГ должна быть предусмотрена система синхронизации с астрономическим точным временем.

Должен выполняться следующий временной регламент:

- интервал опроса аналоговых и дискретных сигналов – не более 100мсек;
- точность хранения меток времени – не хуже 1мсек;
- глубина хранения архивных данных – не менее 3 лет;

- время восстановления работоспособности при переходе на дублирующий сервер – не более 2 секунд.

6.8. Требования к техническому перевооружению системы измерения уровня верхнего и нижнего бьефа.

6.8.1. Требования к системе в целом.

Система измерения верхнего и нижнего бьефа должна:

- быть сертифицирована органами Госстандарта России;
- быть оснащена средствами самодиагностики всех составляющих;
- содержать в своем составе только серийно выпускаемые промышленные контроллеры и программное обеспечение, имеющие в соответствии с законодательством Российской Федерации статус «российское происхождение»;
- использовать для измерения существующие датчики уровня;
- в шкафах должны быть предусмотрены меры для защиты входных сигналов от помех;
- в шкафах должны быть предусмотрены модули гальванической развязки дискретных и аналоговых входных и выходных сигналов (гальваническая развязка входов/выходов диагностических сигналов в пределах шкафа не требуется);
- все источники питания должны иметь электронную защиту от перегрузки и токов короткого замыкания.

6.9. Требования к системе электропитания модернизируемого и нового оборудования.

- система электропитания должна проектироваться в соответствии с «Правилами устройства электроустановок» (ПУЭ) и указанием класса электроприемников;
- система электропитания должна обеспечивать надежное бесперебойное энергоснабжение оборудования переменным напряжением 220В, 50 Гц и постоянным напряжением 220В;
- система электропитания должна обеспечить защиту оборудования от помех в электрической сети, а также временных отключений электроэнергии. Аппаратные и программные решения системы должны исключить риск возможной утраты данных вследствие аварии системы энергоснабжения.

6.10. Требования к модернизации смежных автоматизированных систем.

При невозможности обеспечить при техническом перевооружении АСУГ поддержки существующей структуры каналов и протоколов связи с внешними автоматизированными системами (СВ, ПТК ЭГР, ПТК ССМД, ПТК ЦСМЗ) необходимо выполнить соответствующие проектные работы в отношении данных систем, также предусмотреть необходимые работы по корректировке их аппаратной и программной составляющих.

7. Требования по информационной безопасности

7.1. Основные требования:

7.1.1. По результатам обследования должен быть подготовлен отчет, отражающий информацию о соответствии/несоответствии технологических систем требованиям законодательства о КИИ (если объект не является значимым объектом КИИ к нему применяются требования как значимому объекту КИИ 3 категории значимости или в соответствии с установленным классом защищенности автоматизированной системы управления) с указанием перечня мероприятий, выполнение которых обеспечит соответствие технологических систем требованиям законодательства о КИИ;

7.1.2. Комплект организационно-распорядительной документации должен включать документы различного уровня (регламенты, положения, инструкции) и покрывать

все требования по документированию процессов информационной безопасности, установленные приказами ФСТЭК России №235, №239 по обеспечению безопасности значимых объектов КИИ (По решению субъекта критической информационной инфраструктуры Требования приказа ФСТЭК России №239 могут применяться для обеспечения безопасности объектов критической информационной инфраструктуры, не отнесенных к значимым объектам. Если объект не является значимым объектом КИИ, к нему применяются требования как значимому объекту КИИ 3 категории значимости. Если объект является АСУТП, то в дополнение к требованиям приказа ФСТЭК России №239 должны быть выполнены требования приказа ФСТЭК России №31 в соответствии с установленным классом защищенности автоматизированной системы управления.) и иными нормативными документами, в т.ч. комплект организационно-распорядительной документации должен определять правила и процедуры реализации отдельных организационных и (или) технических мер безопасности (меры изложить подробно с привязкой к конкретному объекту и сопоставлением с разработанными на этапе проекта или уже существующими на объекте и организационными и техническими мерами);

7.1.3. Комплект организационно-распорядительной документации должен включать, но не ограничиваться:

- Политику управления доступом;
- Политику антивирусной защиты;
- Политику резервного копирования;
- Политику осведомленности и обучения персонала в области ИБ;
- Политику обеспечения действий в нештатных ситуациях;
- Регламент управления доступом;
- Регламент обеспечения сетевой безопасности;
- Регламент обеспечения целостности;
- Регламент проведения аудитов безопасности;
- Регламент управления инцидентами ИБ;
- Регламент обеспечения непрерывности;
- Регламент управления обновлениями и уязвимостями;
- Регламент управления изменениями;
- Инструкцию по защите машинных носителей;
- Инструкцию по обеспечению физической защищенности компонентов информационной системы;
- Правила поведения пользователей в информационной системе;
- План мероприятий по обеспечению защиты информации (проект). Приказ о распределении ответственности в области обеспечения безопасности КИИ (назначении подразделения или лица ответственного за обеспечение безопасности значимых объектов КИИ);
- Должностные инструкции лиц ответственных за обеспечение безопасности КИИ или Положение о подразделении ответственным за обеспечение безопасности КИИ;
- Порядок контроля выполнения мероприятий по обеспечению безопасности КИИ;
- Порядок взаимодействия с ГосСОПКА;

7.1.4. Рабочая (эксплуатационная) документация должна содержать:

- описание архитектуры подсистемы безопасности;
- порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации;
- правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации);
- паспорт системы, описывающий окончательное состояние системы на момент установки;

- программу-методику испытаний.

Комплект уточняется на этапе согласования ТЗ.

7.2. Требования к реализуемым защитным мерам технологических сегментов

7.2.1. Должны быть рассмотрены следующие организационные и технические меры защиты технологических сегментов:

- идентификация и аутентификация (ИАФ);
- управление доступом (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации (ЗНИ);
- аудит безопасности (АУД);
- антивирусная защита (АВЗ);
- предотвращение вторжений (компьютерных атак) (СОВ);
- обеспечение целостности (ОЦЛ);
- обеспечение доступности (ОДТ);
- защита технических средств и систем (ЗТС);
- защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
- планирование мероприятий по обеспечению безопасности (ПЛН);
- управление конфигурацией (УКФ);
- управление обновлениями программного обеспечения (ОПО);
- реагирование на инциденты информационной безопасности (ИНЦ);
- обеспечение действий в нештатных ситуациях (ДНС);
- информирование и обучение персонала (ИПО);

7.2.2. Базовый набор мер по обеспечению безопасности может быть адаптирован и дополнен на основании разработанной модели угроз. Набор мер должен быть достаточным для обеспечения безопасности значимого объекта КИИ 3 категории значимости и должен обеспечивать нейтрализацию всех актуальных угроз безопасности информации;

7.2.3. Принимаемые организационные и технические меры должны соотноситься с мерами по промышленной, функциональной безопасности, иными мерами по обеспечению безопасности. При этом меры по обеспечению безопасности не должны оказывать отрицательного влияния на функционирование объекта в проектных режимах его работы;

7.2.4. Требования по информационной безопасности должны быть едиными для всех технологических систем, вне зависимости от того относится данная технологическая система к значимым объектам КИИ или нет.

7.2.5. В проектируемой системе должны быть реализованы и документально описаны следующие процессы:

- Идентификация и аутентификация пользователей и иницируемых ими процессов;
- Идентификация и аутентификация устройств;
- Управление идентификаторами;
- Управление средствами аутентификации;
- Идентификация и аутентификация внешних пользователей;
- Защита аутентификационной информации при передаче;
- Управление учетными записями пользователей;
- Разделение полномочий (ролей) пользователей;
- Назначение минимально необходимых прав и привилегий;
- Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему;

- Блокирование сеанса доступа пользователя при неактивности;
- Управление действиями пользователей до идентификации и аутентификации
- Реализация защищенного удаленного доступа;
- Контроль доступа из внешних информационных (автоматизированных) систем;
- Учет машинных носителей информации;
- Управление физическим доступом к машинным носителям информации;
- Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации;
- Контроль подключения съемных машинных носителей информации;
- Уничтожение (стирание) информации на машинных носителях информации;
- Инвентаризация информационных ресурсов;
- Анализ уязвимостей и их устранение;
- Генерирование временных меток и (или) синхронизация системного времени;
- Регистрация событий безопасности;
- Защита информации о событиях безопасности;
- Мониторинг безопасности;
- Реагирование на сбои при регистрации событий безопасности;
- Реализация антивирусной защиты;
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов);
- Контроль целостности программного обеспечения;
- Резервное копирование информации;
- Обеспечение возможности восстановления информации;
- Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях;
- Контроль предоставляемых вычислительных ресурсов и каналов связи;
- Организация контролируемой зоны;
- Управление физическим доступом;
- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;
- Защита от внешних воздействий;
- Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями;
- Защита периметра информационной (автоматизированной) системы;
- Эшелонированная защита информационной (автоматизированной) системы;
- Организация демилитаризованной зоны;
- Управление сетевыми потоками;
- Скрытие архитектуры и конфигурации информационной (автоматизированной) системы;
- Защита информации при ее передаче по каналам связи;
- Обеспечение доверенных канала, маршрута;
- Запрет несанкционированной удаленной активации периферийных устройств;
- Управление сетевыми соединениями;
- Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;
- Выявление компьютерных инцидентов;
- Информирование о компьютерных инцидентах;
- Анализ компьютерных инцидентов;
- Хранение и защита информации о компьютерных инцидентах;
- Управление изменениями;

- Установка (инсталляция) только разрешенного к использованию программного обеспечения;
- Поиск, получение обновлений программного обеспечения от доверенного источника;
- Контроль целостности обновлений программного обеспечения;
- Тестирование обновлений программного обеспечения;
- Установка обновлений программного обеспечения;
- Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций.

7.3. Требования к методам и средствам обеспечения информационной безопасности в технологических сегментах АСУ ТП

- 7.3.1. В приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства;
- 7.3.2. Проектируемые средства защиты информации должны иметь действующие сертификаты ФСТЭК России и/или ФСБ России;
- 7.3.3. Все проектируемые средства защиты информации не должны оказывать негативного влияния на технологические процессы;
- 7.3.4. Все проектируемые средства защиты информации должны быть обеспечены гарантийной и (или) технической поддержкой на весь период эксплуатации;
- 7.3.5. В случае если в ходе проектирования предусмотрена разработка программного обеспечения, в том числе программного обеспечения средств защиты информации, такая разработка проводится в соответствии со стандартами безопасной разработки программного обеспечения;
- 7.3.6. Должно быть предусмотрено горячее резервирование проектируемого оборудования, непосредственно участвующего в обработке технологической информации, если это допускается технологиями и протоколами работы АСУ ТП. Если горячее резервирование не допускается, должен быть предусмотрен «холодный резерв»;
- 7.3.7. Проектируемые средства защиты информации должны быть согласованы с подразделением информационной безопасности, осуществляющим защиту информации объекта.

7.4. Требования к сегментации технологических сегментов АСУ ТП

- 7.4.1. Взаимодействие между технологическими сетями и корпоративным сегментом (в случае наличия такой необходимости) должно осуществляться с использованием технологии однонаправленной передачи данных (диоды данных);
- 7.4.2. Взаимодействие технологических сетей с сетью Интернет не допускается;
- 7.4.3. Взаимодействие технологических сетей с внешними выделенными сетями должно быть организовано через межсетевой экран с организацией DMZ-зон (используются промежуточные сервера, располагаемые в демилитаризованных зонах);
- 7.4.4. В DMZ размещаются сервера, не имеющие доступа в технологические сегменты. Технологические данные сохраняются на серверах в DMZ путем разрешающих правил со стороны технологической сети. Внешние пользователи взаимодействуют только с данными серверами как с источниками данных. Правила межсетевого экранирования настраиваются для каждого сервера отдельно.

- 7.4.5. Взаимодействие между сетями и сегментами внутри технологических сетей должно осуществляться исключительно через интерфейсы, организованные на межсетевом экране. Исключения из этого правила допускается только по согласованию с ДЗР Эн+ Менеджмент;
- 7.4.6. Каждую технологическую систему необходимо выделить в отдельный сетевой сегмент. В отношении каждой технологической системы обеспечить сегментирование по функциональным уровням (верхний, средний, нижний).
- 7.4.7. Внутри функциональных уровней должно быть обеспечено более детальное сегментирование (микросегментирование). В частности, должны выделяться сегменты для администрирования АРМов и серверов, сегменты для администрирования сетевого оборудования и межсетевых экранов, сегменты для управления и настройки технологических систем и технологического оборудования, сегменты многофункциональных устройств и периферийного оборудования. Микросегментирование осуществляется индивидуально для каждой технологической системы с учетом критичности системы и особенностей ее функционирования.
- 7.4.8. Для обеспечения сетевой безопасности внутри одной подсети должны применяться локальные межсетевые экраны на АРМах, серверах, контроллерах.
- 7.4.9. Сегментирование должно быть проведено таким образом, чтобы исключить возможность доступа между сегментами в обход межсетевого экрана.

8. Этапы реализации

I этап: организационные и проектные работы по техническому перевооружению Автоматизированной системы управления гидроагрегатами Братской ГЭС. Выполнение предпроектного обследования, разработка, обоснование и согласование обобщенного технического задания, модели угроз с Заказчиком, департаментом по эксплуатации "ЕвроСибЭнерго-Гидрогенерация" и ДЗР Эн+ Менеджмент «Сибирь».

II этап: разработка и согласование проектной и рабочей документации с Заказчиком, департаментом по эксплуатации "ЕвроСибЭнерго-Гидрогенерация" и ДЗР Эн+ Менеджмент «Сибирь».

III этап: закупка, изготовление, поставка, монтаж и наладка оборудования для техперевооружения:

- АСУГ укрупненного блока (для ГА ст.№ 1Г, 2Г);
- сетевого оборудования и подсистемы верхнего уровня АСУГ;
- подсистемы измерения уровня верхнего и нижнего бьефа.

IV – XVI этапы: закупка, изготовление, поставка, монтаж и наладка оборудования для техперевооружения АСУГ одиночных блоков (для ГА ст.№ 9 – 18) и укрупненных блоков (для ГА ст.№ 3 – 8), выходящих в плановый капитальный ремонт.

9. Особые условия

- 9.1. Повышенный уровень ответственности.
- 9.2. Действующее предприятие.

10. Дополнительные требования

- 10.1. Основные проектные решения предварительно согласовывать с Заказчиком, департаментом по эксплуатации "ЕвроСибЭнерго-Гидрогенерация" и ДЗР Эн+ Менеджмент «Сибирь».
- 10.2. Сметная документация должна соответствовать «Методики определения стоимости работ по подготовке проектной документации», утвержденной приказом

Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 1 октября 2021 г. № 707/пр., и должна быть выполнена согласно требованиям СТП 907-011.210.032-2020 (приказ от 14.09.2020 №358) «Порядок формирования и утверждения перечня проектно-изыскательских работ, разработки заданий на проектирование, проведения экспертизы и согласования проектно-сметной документации» ООО «ЕвроСибЭнерго-Гидрогенерация», СТП 907-011.202.115-2020 «Ценообразование в ремонтной, строительной деятельности, услуг производственного и непроизводственного (технического) характера» ООО «ЕвроСибЭнерго-Гидрогенерация».

- 10.3. Проектная и рабочая документация при направлении на согласование Заказчику в полном объеме (включая обосновывающие расчеты) предоставляется на бумажном носителе в 3 (трех) экз., в 2 (двух) экземплярах в электронном виде (в формате MS Word, Adobe Acrobat, схемы и графические материалы в редактируемом формате MS Visio) на USB Flash-накопителе.
- 10.4. Не допускается передача документации Заказчику в электронном виде с пофайловым разделением страниц.
- 10.5. Информация, полученная при предпроектном обследовании, проектная, рабочая и конкурсная документации являются конфиденциальной собственностью Заказчика, и передача ее третьим лицам без его согласия запрещается.
- 10.6. При направлении откорректированных материалов проектной и рабочей документации разработчиком должен быть приложен перечень направляемых томов (разделов) с указанием страниц, в которые были внесены изменения. Кроме того, указанные изменения должны быть выделены цветом по тексту документов.
- 10.7. Предусмотреть обучение персонала на специализированных курсах по параметризации оборудования верхнего и нижнего уровня, работе с используемым в автоматизированной системе системным и прикладным ПО в количестве не менее 3 человек.

11. Срок выполнения разработки проектной документации

- 11.1. Срок проведения предпроектного обследования 24.12.2022
- 11.2. Срок разработки и передачи заказчику Технического задания 31.05.2023 г.
- 11.3. Срок передачи раздела проектной и рабочей документации заказчику 25.12.2023 г.
- 11.4. Сроки реализации: начиная с 01.01.2023г. выполнить поставку оборудования, СМР, ПНР согласно графика, разработанного в рамках Рабочей документации, с заключением дополнительных соглашений с учетом годового коэффициента инфляции.

12. Заказчик

Филиал ООО «ЕвроСибЭнерго-Гидрогенерация» «Братская ГЭС».

13. Исходные данные

- 13.1. Исходные данные выдаются по письменному запросу проектной организации.
- 13.2. При проведении работ Заказчик должен предоставить Подрядчику в рамках проведения предпроектного обследования следующую информацию в качестве исходных данных для разработки системы.
 - Схемы для программно-технических комплексов, перечни сигналов, планы объекта и размещения оборудования.
 - Информацию по существующим сетям электропитания и заземления, точкам подключения оборудования, запасам по мощности в точках подключения, характеристикам заземления.
 - Другие необходимые данные для выполнения работ по настоящему Документу.
- 13.3. Подрядчик обязан действовать в соответствии с Соглашением о неразглашении и не

вправе передавать предоставленную Заказчиком в рамках работ информацию третьим лицам без согласия Заказчика.

14. Требования к исполнителю

- 14.1. Подрядчик должен иметь квалифицированный персонал, обладающий дипломами и сертификатами, подтверждающими его квалификацию по направлению «информационная безопасность» и в области обеспечения безопасности технологических систем, а также подтверждающими знание технологических процессов в электроэнергетике.
- 14.2. Наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации и на деятельность по разработке и производству средств защиты конфиденциальной информации.
- 14.3. Исполнитель должен иметь опыт проектирования и реализации не менее 10 (десяти) аналогичных систем, эксплуатируемых в настоящее время на объектах гидрогенерации.
- 14.4. Наличие у организации международного стандарта качества к деятельности по автоматизации технологических процессов и конструированию/производству низковольтных комплектных устройств ГОСТ ISO-9001-2011.
- 14.5. Исполнитель должен иметь собственный положительный опыт применения в аналогичных проектах предлагаемой им номенклатуры технических и программных средств, полностью удовлетворяющих требованиям настоящего задания.

Директор филиала ООО
«ЕвроСибЭнерго-Гидрогенерация»
«Братская ГЭС»

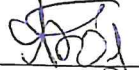


Е.В. Стрелков


Лист согласования к заданию на выполнение комплекса работ по модернизации «Техническое перевооружение автоматизированной системы управления гидроагрегатами Братской ГЭС»

Визы:


Главный инженер Филиала
ООО «ЕвроСибЭнерго-Гидрогенерация»
«Братская ГЭС»


_____ А.В. Боярский
« 12 » 06 2022 г.

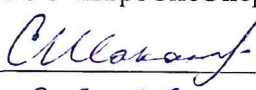
Руководитель департамента
по эксплуатации
ООО «ЕвроСибЭнерго-Гидрогенерация»


_____ Р.В. Берицкий
« 27 » 09 2022 г.


Зам. главного инженера Филиала
ООО «ЕвроСибЭнерго-Гидрогенерация»
«Братская ГЭС»


_____ С.В. Храмушин
« 12 » 09 2022 г.


Начальник ОРЗЭА
департамента по эксплуатации
ООО «ЕвроСибЭнерго-Гидрогенерация»


_____ С.В. Шакалов
« 28 » 09 2022 г.

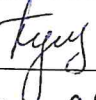
Начальник ЦРЗА Филиала
ООО «ЕвроСибЭнерго-Гидрогенерация»
«Братская ГЭС»


_____ С.Е. Скляров
« 12 » 09 2022 г.


Руководитель департамента АСУТП
АО «ЕвроСибЭнерго»


_____ К.Ю. Малькевич
« » 2022 г.

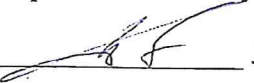
Начальник ОКС Филиала
ООО «ЕвроСибЭнерго-Гидрогенерация»
«Братская ГЭС»


_____ Д.Н. Пушечников
« 12 » 09 2022 г.

Руководитель департамента
по капитальному строительству
ООО «ЕвроСибЭнерго-Гидрогенерация»


_____ М.Ю. Князев
« 27 » 09 2022 г.

Руководитель группы АСУТП
ООО «ЕвроСибЭнерго-Гидрогенерация»
«Братская ГЭС»


_____ Л.Ю. Писарев
« 12 » 09 2022 г.