

«УТВЕРЖДАЮ»
Главный инженер
ООО «ЭН+ ГИДРО КАРЕЛИЯ»
А.О. Тельбухов
« 27 » 2026 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Выполнение проектно-изыскательских работ по объекту «Реконструкция систем автоматического управления и регулирования ГА-1, ГА-2, ГА-3, ГА-4 ОГЭС»

1. Основания для проектирования

- 1.1. Указ Президента РФ от 30 марта 2022 г. N 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».
- 1.2. Постановление Правительства РФ от 14 ноября 2023 г. № 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».

2. Вид строительства

Техническое перевооружение.

3. Основные данные и требования к проектным решениям

- 3.1. Предусмотреть технические решения в соответствии с ОТР (Приложение №1 к настоящему Заданию). Подрядчик может предложить отличные от ОТР решения, принятые решения должны быть обоснованы и согласованы с Заказчиком.

4. Район и площадка строительства

Республика Карелия, Сегежский р-он, д. Каменный Бор, ООО «ЭН+ ГИДРО КАРЕЛИЯ».

5. Этапы и состав выполнения работ

- I этап: выполнение предпроектного обследования, разработка, обоснование и согласование обобщённого технического задания;
- II этап: разработка проектной документации и технических требований к вновь устанавливаемому оборудованию, согласование принятых проектных решений с Заказчиком, департаментом по эксплуатации «ЭН+ ГИДРО», отделом ИБ КИИ и департаментом АСУТП АО «ЭН+ ГЕНЕРАЦИЯ»;
- III этап: разработка рабочей документации и ее согласование с Заказчиком, департаментом по эксплуатации «ЭН+ ГИДРО», отделом ИБ КИИ и департаментом АСУТП АО «ЭН+ ГЕНЕРАЦИЯ».

6. Особые условия

- 6.1. Повышенный уровень ответственности и требования к надежности.
- 6.2. Действующее предприятие.

7. Требования к проектной и рабочей документации

- 7.1. 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 Р 59793-2021, ГОСТ 34.602-2020, ГОСТ 34.201-2020, ГОСТ Р 59795-2021, СТО 59012820.29.020.009-2016, СТП 907-011.210.032-2020 «Порядок формирования и утверждения перечня проектно-изыскательских работ, разработки заданий на проектирование, проведения экспертизы и согласования проектно-сметной документации» ООО «ЕвроСибЭнерго-Гидрогенерация», а также документов, указанных в разделе 2.1 в Приложении №3 к настоящему Заданию.

7.2. Полный объем и требования к проектной и рабочей документации изложены в Приложении №3 к настоящему Заданию.

8. Требования по информационной безопасности

8.1. Предусмотреть технические решения в соответствии с «Требованиями к информационной безопасности» (Приложение №2 к настоящему Заданию). Подрядчик может предложить отличные от ОТР решения, принятые решения должны быть обоснованы и согласованы с Заказчиком.

9. Дополнительные требования

9.1. Сметная документация должна соответствовать «Методике 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 ЭНГ.202.115-2026 «Ценообразование в ремонтной, строительной деятельности, услуг производственного и непроизводственного (технического) характера» ООО «ЭН+ ГИДРО».

9.2. 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.

9.3. Не допускается передача документации Заказчику в электронном виде с пофайловым разделением страниц.

9.4. Информация, полученная при предпроектном обследовании, техническое задание, проектная, рабочая и конкурсная документации являются конфиденциальной собственностью Заказчика, и передача ее третьим лицам без его согласия запрещается.

9.5. 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.

9.6. В сметной документации предусмотреть обучение персонала (инженеры АСУ ТП) на специализированных курсах поставщика оборудования по параметризации оборудования верхнего и нижнего уровня, работе с используемым в автоматизированной системе системным и прикладным ПО в количестве не менее 3 человек.

10. Срок выполнения проекта

10.1. Срок выполнения проекта определяется условиями договора.

11. Заказчик

ООО «ЭН+ ГИДРО КАРЕЛИЯ».

12. Исходные данные

12.1. Приложение №1. Основные технические решения (ОТР) САУ ГА ООО «ЭН+ ГИДРО КАРЕЛИЯ».

12.2. Приложение №2 Требования к информационной безопасности.

12.3. Приложение №3 Требования к проектной и рабочей документации.

12.4. Проектная и эксплуатационная документация на действующие САУ ГА, реализованные на ПТК Siemens.

12.5. Исходные данные выдаются по письменному запросу проектной организации, в срок не более 10 календарных дней.

12.6. При проведении работ Заказчик должен предоставить Подрядчику в рамках проведения предпроектного обследования следующую информацию в качестве исходных данных для разработки системы:

- Проектная документация на существующие программно-технические комплексы.
- 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.

12.7. Подрядчик обязан действовать в соответствии с Соглашением о неразглашении и не вправе передавать предоставленную Заказчиком в рамках работ информацию третьим лицам без согласия Заказчика.

13. Требования к исполнителю

13.1. Участник закупки должен обладать необходимыми трудовыми, материально-техническими

и организационными ресурсами для выполнения работ по настоящему Техническому заданию.

- 13.2.** Участник закупки 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.
- 13.3.** Участник закупки должен иметь в штате либо на основании гражданско-правовых договоров квалифицированных специалистов по направлениям:
- автоматизированные системы управления технологическими процессами;
 - информационная безопасность;
 - проектирование промышленных автоматизированных систем;
 - технологические процессы объектов электроэнергетики.

В подтверждение участник предоставляет:

- справку о кадровом составе;
 - копии документов об образовании ключевых специалистов;
 - копии действующих сертификатов/удостоверений о повышении квалификации (при наличии).
- 13.4.** Участник закупки должен иметь опыт выполнения работ по проектированию, модернизации, внедрению систем автоматизированного управления гидроагрегатами, эксплуатируемых в настоящее время на объектах гидроэнергетики. В подтверждение участник предоставляет: справку об аналогичных договорах, копии актов выполненных работ (не менее 5 проектов или систем).
- 13.5.** Раздел информационной безопасности проекта должен быть разработан организацией, имеющей лицензию ФСТЭК на техническую защиту конфиденциальной информации и иметь опыт работы на рынке услуг в области информационной безопасности не менее 5 лет.
- 13.6.** Участник закупки вправе привлекать соисполнителей для выполнения специализированных работ при условии предоставления сведений о таких организациях и подтверждающих документов об их квалификации и наличии необходимых лицензий.
- 13.7.** Исполнитель должен иметь сертификат системы менеджмента качества ГОСТ Р ИСО 9001-2015 в отношении исследований, разработки, проектирования, производства, испытаний, монтажа, пусконаладочных работ, обслуживания и эксплуатации энергооборудования.
- 13.8.** Предлагаемые исполнителем технические и программные средства должны иметь опыт применения на объектах гидроэнергетики РФ и полностью удовлетворять требованиям настоящего задания.

Начальник ЭТЛ



Клевакин С. И.

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

1. Назначение проведения работ

Реализация работ по техническому перевооружению САУ ГА служит для выполнения следующих задач:

- выполнение требований по обеспечению информационной безопасности объектов критической информационной инфраструктуры Российской Федерации;
- замена оборудования и ПО ПТК САУ ГА, выполнение требований по импортозамещению применительно к электронным компонентам системы и используемому ПО (Постановление Правительства РФ от 14 ноября 2023 г. № 1912);
- сохранение, по возможности, существующих кабельных линий между полевым уровнем и оборудованием ПТК, между САУ ГА и внешними автоматизированными системами (ГРАМ, центральная сигнализация).

2. Описание автоматизированной системы

Система автоматического управления гидроагрегатом (САУ ГА) предназначена для осуществления необходимых технологических операций по управлению турбиной, генератором и их вспомогательным оборудованием при переходных и установившихся режимах работы гидроагрегата на основе результатов контроля состояния его узлов и внешних команд управления. САУ ГА установлены на всех четырех гидроагрегатах ГЭС. САУ ГА реализованы на ПТК Siemens.

САУ ГА №1-3 являются значимыми объектами критической информационной структуры и имеют 3 категорию значимости.

Техническому перевооружению, согласно настоящему техническому заданию, подвергаются все 4 системы.

2.1. Состав системы

- подсистема технологической автоматики (ТА);
- подсистема автоматического регулирования частоты и активной мощности (АРЧМ);
- подсистема термоконтроля;
- подсистема управления вспомогательным оборудованием (УВО);
- информационная подсистема.

2.1.1. Подсистема ТА, обеспечивает управление исполнительными устройствами основного оборудования гидроагрегата на основе информации о его состоянии и внешних команд управления.

2.1.2. Подсистема АРЧМ (РЧВ) предназначена для выполнения функций регулирования частоты и активной мощности гидроагрегата с помощью гидромеханической части системы регулирования гидротурбины, а также для управления открытием регулирующих органов турбины в переходных режимах работы гидроагрегата, обеспечение устойчивой работы агрегата в сети на индивидуальном и групповом регулировании, выполнение гарантий регулирования при сбросах нагрузки.

2.1.3. Подсистема термоконтроля формирует сигналы аварийной остановки, предупредительной и аварийной сигнализации при достижении температуры выставленных уставок.

2.1.4. Подсистема УВО предназначена для управления вспомогательным оборудованием агрегата, обеспечивающим готовность к пуску и нормальную его работу во всех режимах.

2.1.5. Информационная подсистема предназначена для отображения и изменения параметров системы управления, текущих значений параметров агрегата, положения коммутационных аппаратов и исполнительных устройств, режима работы агрегата и команд управления в виде мнемосхем и графиков, запись в журнал событий с расшифровкой предупредительной и аварийной сигнализации о работе основного и вспомогательного оборудования, а также возможность обмена данными по цифровым интерфейсам.

2.2. Функции, выполняемые системой автоматического управления гидроагрегатом

- контроль параметров агрегата и связанного оборудования;
- работа агрегата на холостом ходу;
- автоматический и ручной пуск гидроагрегата;
- ручная точная, автоматическая точная, самосинхронизация гидроагрегата для включения в сеть;
- ручное и автоматическое управление нагрузкой гидроагрегата;
- работа агрегата в режиме синхронного компенсатора;
- останов гидроагрегата (ручной, автоматический и аварийный при работе защит);
- гидромеханические защиты агрегата;
- управление быстропадающими щитами;
- обмен информацией с действующей системой верхнего уровня, реализованной с помощью контроллеров Simatic.

2.3. Система автоматического управления гидроагрегатом должна

- воспроизводить алгоритмы работы действующих САУ ГА, реализованных на ПТК Siemens;
- в отношении ПТК и компонентов, быть сертифицирована органами Госстандарта России, иметь сертификат соответствия Техническим регламентам РФ и/или Таможенного Союза и внесены в Федеральный информационный фонд по обеспечению единства измерений в качестве технических средств, рекомендуемых к применению в энергетической отрасли;
- соответствовать требованиям Постановления Правительства РФ от 14 ноября 2023 г. № 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»;
- быть дублирована и оснащена средствами самодиагностики всех составляющих;
- все проектируемые программно-аппаратные комплексы и/или программно-аппаратные средства должны быть отечественного производства (сведения о программно-аппаратных комплексах и/или программно-аппаратных средствах должны содержаться в реестре российской промышленной продукции).
- программное обеспечение, используемое в составе проектируемых программно-аппаратных комплексов (и/или программно-аппаратных средств), должно быть включено в единый реестр российских программ для электронных вычислительных машин и баз данных.
- 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;
- все источники питания должны иметь электронную защиту от перегрузки и токов короткого замыкания;
- в результате предпроектного обследования должен быть сформирован дополнительный перечень точек измерения, необходимый для организации эффективной и безопасной работы САУ ГА и смежных с ней систем, с выбором удовлетворяющих поставленной задаче мест установки и монтажом дополнительного оборудования и датчиков;
- разработать проектные решения по замене существующих пропорциональных гидрораспределителей, установленных в гидромеханической колонке, на аналоги общепромышленного типа, марку и тип проектных пропорциональных гидрораспределителей необходимо согласовать с заказчиком, указанные проектные решения не должны приводить к замене остального оборудования гидромеханической колонки или гидравлической системы регулирования;
- ориентировочное количество входных-выходных сигналов должно составлять не менее:
- аналоговых входных сигналов (4...20 мА / -10...+10 В) – 25;
- аналоговых входных сигналов (RTD) – 45;
- аналоговых выходных сигналов (4...20 мА / -10...+10 В) – 10 (из них с управляющими воздействиями – 2);
- дискретных входных сигналов – 110;

- дискретных выходных сигналов – 45 (из них с управляющими воздействиями – 27);
- цифровой сигнал – 10;
- должен быть предусмотрен 10% резерв по каналам управления и контроля.
- объем и состав комплекта расходных материалов, приспособлений, инструментов и запасных частей должен быть достаточным для надежной и безотказной эксплуатации САР в течение гарантийного срока и составлять не менее чем 20% от общего количества элементов системы каждого типа, но не менее 1 штуки.

2.4. Требования к конструктивному исполнению

- шкафы с одной операторской панелью, стандартных габаритов (ШхВхГ) 800х2000х600 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;
- 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;
- для обеспечения удобства обслуживания шкафов в них должно быть предусмотрено освещение и оснащение розеткой на ~220В, подключенной к отдельному автоматическому выключателю номиналом не менее 6А. Включение освещения должно происходить при открывании дверей шкафа, а также предусмотрены ручные выключатели;
- на шкафах на лицевой и обратной стороне необходимо разместить надписи (таблички с надписью), соответствующие номеру шкафа и его наименованию;
- цвет окраски шкафов RAL 7035.

2.5. Требования по стандартизации и унификации

- 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.
- в ПТК должно использоваться минимальное количество питающих напряжений;
- номенклатура используемых конструктивных единиц должна быть сведена к минимуму. 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 установленного ряда шкафов, в который будет устанавливаться шкаф САУ ГА;
- формы представления информации оператору должны быть приближены к проектным изображениям технологических схем и их элементов;
- в ПТК должны применяться программируемые логические контроллеры одного производителя;
- программно-технические средства системы САУ ГА должны быть серийно выпускаемыми. Не допускается применение морально устаревших технических средств, а также уникальных устройств.

2.6. 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. Эта замена должна осуществляться, как правило, в «горячем» режиме (без прерывания работы системы) и не должна приводить к внесению каких-либо изменений или перестройке других технических средств;

- САУ ГА должна обеспечить управление, как в автоматическом, так и в ручном режиме работы;
- нижний уровень САУ ГА должен быть реализован на двух резервированных контроллерах, каждый из которых содержит полный набор функций, необходимый для управления агрегатом. Контроллеры и модули контроллеров должны иметь исполнение, предусматривающее возможность горячей замены без отключения ГА от сети;
- верхний уровень 4-х САУ ГА должен быть реализован на двух резервированных серверах, двух АРМ операторов и одного АРМ инженерная станция;
- верхний уровень должен быть оснащен оборудованием синхронизации системного времени (GPS/ГЛОНАСС) либо подключен к существующей системе единого времени. Технические решения необходимо определить и согласовать на этапе проектирования;
- устройства САУ ГА должны являться самодостаточной частью АСУ ТП. При исчезновении связи с верхним уровнем система управления должна продолжать функционировать в режиме местного управления с хранением в локальном хранилище всех параметров с глубиной архива не менее 30 дней, с возможностью передачи этих данных на верхний уровень при восстановлении связи.

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

- сохранение физических (по кабельным связям) сигналов управления с ГЦУ – сигналы управления регулятором скорости (всего 2 шт.);
- сохранение существующих обобщенных сигналов срабатывания сигнализации устройств РЗА (вторичных устройств) генератора в центральную сигнализацию;
- в САУ ГА необходимо предусмотреть резервирование гидромеханических защит и управления агрегатом;
- с помощью операторских панелей должна быть обеспечена возможность контроля и управления гидроагрегатом.

2.7. 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.

2.8. Требования к взаимодействию со смежными автоматизированными системами

При техническом перевооружении САУ ГА необходимо обеспечить поддержку существующей структуры каналов и протоколов связи с внешними автоматизированными системами (ГРАМ, центральная сигнализация), в случае невозможности необходимо выполнить соответствующие проектные работы в отношении данных систем, также предусмотреть необходимые работы по корректировке их аппаратной и программной составляющих, если потребуется. Необходимый объем и протоколы информационного обмена между существующим ГРАМ и проектируемым верхним уровнем САУГА определить и согласовать на этапе обследования.

Приложение № 2
к Техническому заданию на выполнение комплекса работ по объекту
«Техническое перевооружение системы автоматического управления
гидроагрегатов (САУ ГА) ООО «ЭН+ ГИДРО КАРЕЛИЯ»

Требования к информационной безопасности

1. Требования к перечню мер по обеспечению безопасности

1.1. В процессе проектирования СОИБ должен быть реализован базовый набор мер по обеспечению безопасности объектов защиты, который определяется на основе установленной категории ЗОКИИ в соответствии с приложением к Приказу ФСТЭК России №239 от 25.12.2017 г.

1.2. Базовый набор мер по обеспечению безопасности объекта защиты подлежит адаптации в соответствии с актуальными угрозами безопасности информации, определёнными в «Модели угроз», разработанной согласно «Методике оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021). При адаптации учитываются применяемые информационные технологии и особенности функционирования ОКИИ.

1.3. Требования к мерам защиты информации для ЗОКИИ 3-й категории приведены в таблице 1. Данный перечень неограничен и может быть уточнен на этапе проектирования СОИБ.

Таблица 1 – Перечень мер защиты для ЗОКИИ 3 категории значимости

Мера	Наименование
I. Идентификация и аутентификация (ИАФ)	
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации
ИАФ.1	Идентификация и аутентификация пользователей и иницируемых ими процессов
ИАФ.2	Идентификация и аутентификация устройств
ИАФ.3	Управление идентификаторами
ИАФ.4	Управление средствами аутентификации
ИАФ.5	Идентификация и аутентификация внешних пользователей
ИАФ.7	Защита аутентификационной информации при передаче
II. Управление доступом (УПД)	
УПД.0	Регламентация правил и процедур управления доступом
УПД.1	Управление учетными записями пользователей
УПД.2	Реализация модели управления доступом
УПД.4	Разделение полномочий (ролей) пользователей
УПД.5	Назначение минимально необходимых прав и привилегий
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему
УПД.10	Блокирование сеанса доступа пользователя при неактивности
УПД.11	Управление действиями пользователей до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление физическим доступом к машинным носителям информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации
ЗНИ.7	Контроль подключения съемных машинных носителей информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации

V. Аудит безопасности (АУД)	
АУД.0	Регламентация правил и процедур аудита безопасности
АУД.1	Инвентаризация информационных ресурсов
АУД.2	Анализ уязвимостей и их устранение
АУД.3	Генерирование временных меток и (или) синхронизация системного времени
АУД.4	Регистрация событий безопасности
АУД.6	Защита информации о событиях безопасности
АУД.7	Мониторинг безопасности
АУД.8	Реагирование на сбои при регистрации событий безопасности
АУД.10	Проведение внутренних аудитов
VI. Антивирусная защита (АВЗ)	
АВЗ.0	Регламентация правил и процедур антивирусной защиты
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Антивирусная защита электронной почты и иных сервисов
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Обеспечение целостности (ОЦЛ)	
ОЦЛ.0	Регламентация правил и процедур обеспечения целостности
ОЦЛ.1	Контроль целостности программного обеспечения
IX. Обеспечение доступности (ОДТ)	
ОДТ.0	Регламентация правил и процедур обеспечения доступности
ОДТ.4	Резервное копирование информации
ОДТ.5	Обеспечение возможности восстановления информации
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи
X. Защита технических средств и систем (ЗТС)	
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем
ЗТС.2	Организация контролируемой зоны
ЗТС.3	Управление физическим доступом
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
ЗТС.5	Защита от внешних воздействий
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	
ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями
ЗИС.2	Защита периметра информационной (автоматизированной) системы
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы
ЗИС.5	Организация демилитаризованной зоны
ЗИС.6	Управление сетевыми потоками
ЗИС.8	Соккрытие архитектуры и конфигурации информационной (автоматизированной) системы
ЗИС.19	Защита информации при ее передаче по каналам связи
ЗИС.20	Обеспечение доверенных канала, маршрута
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств
ЗИС.32	Защита беспроводных соединений
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)
ЗИС.35	Управление сетевыми соединениями
ЗИС.38	Защита информации при использовании мобильных устройств
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных

ХII. Реагирование на компьютерные инциденты (ИНЦ)	
ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты
ИНЦ.1	Выявление компьютерных инцидентов
ИНЦ.2	Информирование о компьютерных инцидентах
ИНЦ.3	Анализ компьютерных инцидентов
ИНЦ.4	Устранение последствий компьютерных инцидентов
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах
ХIII. Управление конфигурацией (УКФ)	
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы
УКФ.2	Управление изменениями
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения
ХIV. Управление обновлениями программного обеспечения (ОПО)	
ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника
ОПО.2	Контроль целостности обновлений программного обеспечения
ОПО.3	Тестирование обновлений программного обеспечения
ОПО.4	Установка обновлений программного обеспечения
ХV. Планирование мероприятий по обеспечению безопасности (ПЛН)	
ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации
ХVI. Обеспечение действий в нештатных ситуациях (ДНС)	
ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях
ДНС.1	Разработка плана действий в нештатных ситуациях
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения
ХVII. Информирование и обучение персонала (ИПО)	
ИПО.0	Регламентация правил и процедур информирования и обучения персонала
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы
ИПО.2	Обучение персонала правилам безопасной работы
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы

1.4. Меры по обеспечению безопасности дополнительно должны обеспечивать нейтрализацию предполагаемых (актуальных) угроз, приведенных в документе «Модель угроз». В случае необходимости перечень мер по обеспечению безопасности, приведенный выше, должен быть уточнен на стадии проектирования.

1.5. Если ЗОКIIИ присвоена категория выше 3-й, то состав защитных мер из таблицы 1, должен быть расширен в соответствии с требованиями приказа ФСТЭК России от 25.12.2017 № 239.

1.6. В случае невозможности технической реализации отдельных выбранных мер, а также с учетом экономической целесообразности должны быть разработаны иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности информации с обоснованием применения компенсирующих мер и согласованием отдела безопасности КИИ АО «ЭН+ ГЕНЕРАЦИЯ».

2. Требования к регламентации мер по обеспечению безопасности

2.1. Организационно-распорядительная документация должна соответствовать требованиям законодательства РФ, локальных нормативных документов Заказчика, нормативно-методических документов Регуляторов (ФСТЭК России и ФСБ России).

2.2. Положения организационно-распорядительных документов по обеспечению безопасности ЗОКИИ должны:

- носить не рекомендательный, а обязательный характер;
- быть выполнимыми и контролируруемыми. Не допускается включать в состав данных документов положения, контроль реализации которых затруднен или невозможен;

- соответствовать требованиям и условиям деятельности субъекта;

2.3. Организационно-распорядительная документация должна регламентировать:

- идентификацию и аутентификацию (ИАФ);
- управление доступа (УПД);
- ограничение программной среды (ОПС)
- защиту машинных носителей информации (ЗНИ);
- аудит безопасности (АУД);
- антивирусную защиту (АВЗ);
- обеспечение целостности (ОЦЛ);
- обеспечение доступности (ОДТ);
- защиту технических средств и систем (ЗТС);
- защиту информационной (автоматизированной) системы и ее компонентов (ЗИС);
- реагирование на компьютерные инциденты (ИНЦ);
- управление конфигурацией информационной (автоматизированной) системы (УКФ);
- управление обновлениями программного обеспечения (ОПО);
- планирование мероприятий по обеспечению защиты информации (ПЛН);
- обеспечение действий в нештатных ситуациях (ДНС);
- информирование и обучение персонала (ИПО).

3. Требования к Системе

3.1. Требования к структуре и функционированию Системы

3.1.1. Требования к защите средств и систем, обеспечивающих функционирование значимых объектов КИИ (обеспечивающей инфраструктуры), определяются в техническом задании на создание системы безопасности такого объекта в соответствии с требованиями, установленными подпунктом «з» пункта 10 Приказа ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

3.1.2. Технические меры защиты должны реализовываться посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

3.1.3. Система обеспечения информационной безопасности (СОИБ) должна являться неотъемлемой составной частью (подсистемой) ОКИИ на всех этапах его жизненного цикла: проектирование, создание, ввод в эксплуатацию, эксплуатация и вывод из эксплуатации.

3.1.4. При проектировании СОИБ рекомендуется руководствоваться принципом «Security by Design», что подразумевает:

- Интеграцию требований и мер защиты информации непосредственно в архитектуру ОКИИ, а не их последующее «добавление» к уже функционирующей системе (при создании новой системы).
- Невозможность реализации производственных и технологических процессов ОКИИ в обход мер защиты, предусмотренных СОИБ.
- Учет рисков информационной безопасности на ранних стадиях проектирования технологических решений.
- Обеспечение встроенных механизмов защиты во все критические компоненты ОКИИ (включая АСУ ТП, сетевое оборудование, серверное и прикладное ПО) при наличии технической возможности.

3.1.5. Все проектные решения в отношении ОКИИ должны разрабатываться с учетом функционирования СОИБ как в штатных режимах, так и в условиях возникновения инцидентов информационной безопасности, не допуская снижения уровня защищенности при изменении конфигурации или состава оборудования.

3.1.6. Должны применяться СЗИ, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки в соответствии с законодательством РФ.

3.1.7. Принимаемые организационные и технические меры защиты информации:

- должны обеспечивать доступность обрабатываемой в ОКИИ информации (исключение неправомерного блокирования), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также при необходимости конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации);
- должны соотноситься с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности;
- должны исключать избыточность в случае, если принятые меры по обеспечению промышленной безопасности и (или) физической безопасности достаточны для блокирования (нейтрализации) отдельных угроз безопасности информации;
- должны учитывать корпоративные требования ГК ЭН+ в части унификации средств защиты информации;
- не должны оказывать отрицательного влияния на штатный режим функционирования АСУ.

3.1.8. С учетом подлежащих реализации мер обеспечения безопасности в состав СОИБ должны входить следующие подсистемы:

- Подсистема сбора событий информационной безопасности;
- Подсистема обеспечения однонаправленной передачи данных;
- Подсистема межсетевого экранирования;
- Подсистема управления доступом;
- Подсистема анализа защищенности информации;
- Подсистема антивирусной защиты;
- Подсистема резервного копирования.

3.1.9. Должны быть реализованы организационные и технические меры по контролю целостности и неизменности программного обеспечения, конфигураций оборудования и средств защиты информации в технологическом сегменте.

3.1.10. В случае необходимости организации удаленного доступа к компонентам технологического сегмента с функциями управления при невозможности физического присутствия на производственной площадке, допускается создание канала временной физической коммутации после согласования с руководством субъекта КИИ и отделом безопасности КИИ. Удаленный доступ допускается только для целей администрирования сетевого оборудования и средств защиты информации (СЗИ) при соблюдении следующих условий:

- Удаленный доступ к компонентам технологического сегмента должен осуществляться исключительно через систему управления привилегированным доступом (РАМ-систему), сертифицированную ФСТЭК России.
- Для защиты канала связи на внешнем периметре используются сертифицированные ФСТЭК России средства криптографической защиты информации (VPN) и/или каналы временной физической коммутации сети. После установки соединения трафик должен направляться на РАМ-систему, исключая прямое сетевое взаимодействие с целевыми ресурсами.
- РАМ-система размещается в корпоративном или изолированном сегменте (со строгим контролем ACL), и обеспечивает проксирование сессий к целевым ресурсам. Допускается использование выделенных узлов удаленного доступа (jump-host) в качестве шлюзов, управляемых РАМ-системой.
- Применяется многофакторная аутентификация для всех пользователей, осуществляющих удаленный доступ (на уровне РАМ).
- Обеспечивается регистрация всех действий администратора (включая видеофиксацию сессий средствами РАМ) с передачей журналов в подсистему сбора событий (п. 4.4.1).
- Запрещается удаленный доступ к компонентам технологического сегмента для лиц, не являющихся работниками субъекта критической информационной инфраструктуры, а также

работниками его дочерних и зависимых обществ.

3.1.11. Подсистема сбора событий информационной безопасности предназначена для централизованного сбора, защиты событий безопасности, а также мониторинг сбоев поступления событий безопасности.

3.1.12. Подсистема однонаправленной передачи данных, используется в технологических сетях с управляющим воздействием для целей передачи данных мониторинга (телеметрии, диагностической информации, журналов событий) из технологического сегмента в корпоративный сегмент (или иные внешние сети) на базе сертифицированных ФСТЭК России диодов данных.

3.1.13. Диод данных реализует аппаратную однонаправленность передачи, что исключает возможность передачи любых данных (управляющих команд, обновлений программного обеспечения, конфигурационных файлов) из корпоративного сегмента (или иных внешних сетей) в технологический сегмент на физическом уровне.

3.1.14. В случае наличия обоснованной технологической необходимости двунаправленного информационного обмена между технологическим сегментом и внешними сетями, должен использоваться отдельный защищённый канал связи, организованный с применением сертифицированных ФСТЭК России средств межсетевого экранирования (тип А, Д) и/или криптографической защиты информации (VPN). При этом:

- Организация каналов с системным оператором производится в соответствии с техническими условиями на подключение и ГОСТ Р 71077—2023 «Дистанционное управление. Правила применения защищенных протоколов при организации информационного обмена.».

- Если в технических условиях организации канала с системным оператором не заложены требования об использовании сертифицированных средств защиты информации (МСЭ, VPN), необходима проработка компенсирующих мер безопасности и согласование изменений с отделом безопасности КИИ АО «ЭН+ ГЕНЕРАЦИЯ».

- Передаваемые в технологический сегмент команды и данные должны быть строго ограничены утверждённым перечнем, подвергаться проверке на уровне прикладных протоколов (включая анализ промышленных протоколов средствами NGFW) и регистрироваться в подсистеме сбора событий безопасности (п. 4.4.1).

3.1.15. Подсистема межсетевого экранирования предназначена для обеспечения управления информационными потоками между устройствами, сетевыми сегментами и информационными (автоматизированными) системами.

3.1.16. Должно быть обеспечено сегментирование технологических сетей в соответствии со следующими принципами:

- каждая технологическая система выделяется в отдельный сетевой сегмент;
- внутри системы сегменты разделяются по функциональным уровням (верхний – АРМ и серверы, средний – контроллеры, нижний – полевые устройства);
- внутри функциональных уровней реализуется микросегментирование (сегменты администрирования, управления оборудованием, телефонии, периферийных устройств и т.п.).

Взаимодействие технологических сетей с сетью Интернет не допускается.

3.1.17. Для защиты от угроз безопасности внутри подсетей дополнительно применяются локальные межсетевые экраны на автоматизированных рабочих местах, серверах и контроллерах (Linux: iptables, ufw, nftables, Windows: брандмауэр).

3.1.18. Подсистема управления доступом предназначена для контроля и управления доступом субъектов доступа к объектам доступа.

3.1.19. Подсистема анализа защищенности информации предназначена для обеспечения проведения систематических мероприятий по анализу защищенности автоматизированной системы и тестированию работоспособности системы ЗИ.

3.1.20. Подсистема антивирусной защиты предназначена для обеспечения обнаружения компьютерных программ, либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

3.1.21. Подсистема резервного копирования предназначена для обеспечения возможности восстановления автоматизированной системы управления в нештатных ситуациях.

3.1.22. Структура СОИБ должна обеспечивать реализацию функций безопасности на всех технологических этапах эксплуатации, в том числе при проведении технического обслуживания и ремонта.

3.1.23. Должны быть предусмотрены следующие режимы функционирования СОИБ:

- штатный режим;
- сервисный режим;
- аварийный режим.

Штатный режим функционирования предусматривает круглосуточное непрерывное функционирование и обеспечение выполнения всех функций Системы.

Сервисный режим функционирования предусматривает проведение регулярного планового обслуживания Системы без прерывания ее функционирования, но с понижением общей производительности на период обслуживания, или с прерыванием функционирования на период планового обслуживания Системы, а также проведение внеплановых ремонтно-восстановительных мероприятий в случае аварий и нештатного функционирования Системы.

Аварийный режим характеризуется отказом одного или нескольких компонент программного и (или) технического обеспечения Системы, и, как следствие, невозможностью выполнения Системой предусмотренных функций в полном объеме. В случае перехода Системы в аварийный режим необходимо выполнить комплекс мероприятий по переходу в сервисный режим и устранению причины аварии:

- диагностирование инцидентов или проблем, связанных либо со сбоями или авариями в работе Системы, либо с попытками НСД к ресурсам сети;
- оперативное противодействие попыткам НСД;
- восстановление при необходимости программно-аппаратной конфигурации Системы (сетевое и серверного оборудования, СЗИ);
- восстановление информации при ее утере средствами системы резервного копирования и восстановления;
- расследование причин НСД или аварии и определение источника инцидента или проблемы (возможно, с привлечением экспертных организаций и правоохранительных органов);
- корректировку механизмов защиты и обеспечения надежности на организационном и программно-техническом уровнях в целях недопущения повторного НСД или аварии.

При успешном окончании сервисного режима (прохождении всех тестов и проверок по функционированию) Система должна переводиться в основной режим функционирования.

3.1.24. Эксплуатация Системы должна предполагать круглосуточный режим работы персонала.

3.1.25. В Системе должны быть предусмотрены механизмы диагностирования состояния и результатов работы компонентов Системы

3.1.26. Состав подсистем может быть дополнен и должен быть уточнен на стадии проектирования и согласован с отделом безопасности КИИ АО «ЭН+ ГЕНЕРАЦИЯ».

3.2. Требования к проектируемым ТС, ПО и СЗИ

3.2.1. Технические меры ЗИ реализуются посредством применения СЗИ, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. Для реализации мер защиты ИБ в качестве СЗИ в первую очередь подлежат рассмотрению механизмы защиты (параметры настройки) штатного программного обеспечения автоматизированной системы управления при их наличии.

3.2.2. В случае принятия решения о применении сертифицированных средств защиты информации должны использоваться СЗИ с уровнем доверия, не ниже установленного нормативными требованиями ФСТЭК России для соответствующего класса систем.

3.2.3. Все проектируемые средства защиты информации должны иметь действующие сертификаты ФСТЭК России и/или ФСБ России. Копии сертификатов предоставляются Заказчику на этапе рабочего проектирования.

3.2.4. Проектируемые средства защиты информации подлежат обязательному согласованию с отделом безопасности КИИ АО «ЭН+ ГЕНЕРАЦИЯ» на стадии проектирования.

3.2.5. Классы защиты и уровни доверия определяются в соответствии с нормативными правовыми актами ФСТЭК России, устанавливающими требования к системам защиты информации (Приказы ФСТЭК России: № 31, № 239), изданными в пределах полномочий, предусмотренных Положением о Федеральной службе по техническому и экспортному контролю (утв. Указом Президента РФ от 16.08.2004 № 1085).

3.2.6. ТС Системы и СЗИ в ее составе должны иметь возможность масштабирования и наращивания функционала путем приобретения дополнительных лицензий и создания (модернизации) подсистем.

3.3. Требования к численности и квалификации персонала и режиму его работы

3.3.1. На стадии проектирования должны быть определены меры обеспечения безопасности ЗОКИИ. Должны быть разработаны решения по численности, квалификации и функциям персонала Системы, режимам его работы, порядку взаимодействия.

3.3.2. В Системе могут быть предусмотрены следующие варианты обеспечения безопасности:

- Структурное подразделение, ответственное за обеспечение безопасности ЗОКИИ.
- Отдельные работники, ответственные за обеспечение безопасности ЗОКИИ (специалисты по безопасности).
- В подразделениях, эксплуатирующих ЗОКИИ, могут также назначаться работники, не связанные с защитой ЗОКИИ, на которых возлагаются отдельные функции по обеспечению безопасности ЗОКИИ.

3.3.3. При этом не допускается возложение на структурное подразделение по безопасности, специалистов по безопасности функций, не связанных с обеспечением безопасности ЗОКИИ. Назначение работников из состава ИБ ДЗР по направлению КИИ, допускается по согласованию с управлением по информационной безопасности «ДЗР Сибирь».

3.3.4. В Системе должно быть предусмотрено наличие персонала минимум со следующими ролями:

- администратора Системы;
- администратор безопасности информации.

3.3.5. Администратор Системы должен обладать навыками эксплуатации ТС и ПО Системы, а его квалификация должна позволять ему обеспечивать функционирование Системы, проводить обслуживание и своевременно реагировать на инциденты, связанные с нарушением функционирования Системы.

3.3.6. Администратор безопасности информации должен обладать знаниями в области обеспечения безопасности информации и навыками в объеме, необходимом для выполнения своих обязанностей при работе с СЗИ в составе Системы, а его квалификация должна позволять ему поддерживать необходимый уровень безопасности информации ИС во всех возможных режимах функционирования.

3.3.7. Численность персонала Системы должна определяться в зависимости от сложности подсистем на стадии проектирования Системы.

3.3.8. Не допускается объединение в одном лице нескольких ролей, указанных в пункте 0.

3.4. Требования к надежности

3.4.1. Программно-аппаратные компоненты в составе подсистем проектируемой Системы должны позволять осуществлять ее резервирование и восстановление после сбоев.

3.4.2. Должна быть обеспечена возможность обнаружения и локализации отказов функционирования компонентов Системы.

3.4.3. Компоненты в составе подсистем проектируемой Системы должны обеспечивать возможность резервного копирования конфигураций и журналов регистрации событий.

3.4.4. Аппаратные компоненты СЗИ в составе проектируемой Системы должны обеспечивать круглосуточную работу.

3.4.5. Система должна обеспечивать возможность непрерывной работы с учетом перерывов, необходимых для технического обслуживания.

Выбор конкретного способа обеспечения отказоустойчивости производится Исполнителем на стадии технического проектирования.

3.5. Требования безопасности

3.5.1. Средства Системы должны обеспечивать идентификацию и аутентификацию персонала по уникальному идентификатору и паролю, сложность и длина которого должна определяться внутренними НПА или рекомендациями ФСТЭК России. При возможности рассматривается реализация с использованием двухфакторной (мультифакторной) аутентификации.

3.5.2. Должна быть реализована модель ролевого доступа, обеспечивающая возможность разрешения или запрета выполнения персоналом Системы заданных операций.

3.5.3. Все используемые в целях создания и развития Системы технические средства должны отвечать требованиям норм технической безопасности, установленных российским законодательством.

3.5.4. На всем жизненном цикле Система должна обеспечивать соблюдение требований охраны труда в соответствии с законодательством Российской Федерации.

3.6. Требования к эргономике и технической эстетике

3.6.1. Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав Системы, должно осуществляться посредством графического пользовательского интерфейса (GUI).

3.6.2. В любом окне графического пользовательского интерфейса должно быть реализовано отображение на экране только тех возможностей, которые доступны конкретному пользователю в соответствии с его функциональной ролью в Системе.

3.6.3. Графический пользовательский интерфейс средств Системы должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм.

3.6.4. Серверные компоненты, аппаратно-программные комплексы защиты информации и активное сетевое оборудование Системы должны иметь возможность установки в стандартные монтажные стойки Заказчика.

3.7. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов

3.7.1. При проектировании Системы должны использоваться унифицированные, однотипные компоненты в целях обеспечения снижения расходов на обслуживание и ремонт, удобства эксплуатации.

3.7.2. Эксплуатация программно-технических средств должна предусматривать следующие виды технического обслуживания:

- оперативное обслуживание;
- профилактические работы.

3.7.3. Оперативное обслуживание должно предусматривать ежедневный контроль функционирования аппаратно-технических средств, целостности ресурсов Системы. Оперативное обслуживание не должно нарушать выполнение функций Системы в целом.

3.7.4. Профилактические работы должны включать в себя периодическую проверку и обслуживание ТС Системы, для которых такое обслуживание и процедуры предусмотрены эксплуатационной документацией.

3.7.5. Объем и порядок выполнения технического обслуживания технических и программных средств Системы должны определяться эксплуатационной документацией на СЗИ.

3.7.6. Физический доступ лиц к сетевому, серверному оборудованию и СЗИ должен осуществляться в соответствии с существующей в организации системой контроля доступа персонала в серверные помещения.

3.8. Требования к защите информации от несанкционированного доступа

3.8.1. Административный доступ к ресурсам Системы должны получать только уполномоченные работники из числа персонала Оператора с использованием СЗИ, позволяющих обеспечить надлежащий уровень конфиденциальности как при локальном, так и при удаленном подключении в границах технологического сегмента. Для подключения к Системе из внешних сегментов (по отношению к технологическому), необходима организация шифрованного, контролируемого канала, согласованного с отделом безопасности КИИ АО «ЭН+ ГЕНЕРАЦИЯ».

3.8.2. Должны быть обеспечены контроль и управление физическим доступом к СЗИ Системы, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к этим средствам.

3.8.3. ЗИ от несанкционированного доступа в Системе должна в том числе обеспечиваться комплексом мер ЗИ от несанкционированного доступа.

3.8.4. ЗИ от несанкционированного доступа Системы должна обеспечиваться на всем жизненном цикле и во всех режимах ее функционирования.

3.8.5. Информация о событиях безопасности и инцидентах, зарегистрированных в Системе, должна передаваться в (SOC) Заказчика (при наличии).

3.8.6. Должны осуществляться регистрация и учет событий ИБ встроенными в СЗИ механизмами журналирования с периодом хранения не менее 1 года.

3.9. Требования по сохранности информации при авариях

3.9.1. При авариях и сбоях Система должна обеспечивать возможность восстановления настроек компонентов из их резервных копий.

3.9.2. Должны быть предусмотрены средства восстановления, обеспечивающие хранение не менее двух резервных копий программных компонентов СЗИ, их регулярную актуализацию и проверку целостности и работоспособности. Должна обеспечиваться сохранность следующей информации:

- аутентификационная информация (пароли, имена учетных записей);
- конфигурационная информация;
- информация о событиях безопасности;
- информация о состоянии и работе компонентов Системы.

3.9.3. Должна обеспечиваться сохранность информации в следующих случаях:

- аварийное завершение функционирования Системы;
- отказ ТС Системы;
- потеря питания;
- компьютерная атака;
- потеря подключения к информационно-телекоммуникационной сети Заказчика или потеря подключения между компонентами Системы и смежными системами.

3.10. Требования к защите от влияния внешних воздействий

3.10.1. Защита от влияния внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) должна обеспечиваться за счет существующих подсистем инженерной инфраструктуры Заказчика.

3.10.2. Помещения, в которых проектируется размещение критически важных технических средств, должны быть оборудованы средствами контроля и управления доступом, пожарной безопасности, видеонаблюдения, вентиляции и кондиционирования. Доступ в такие помещения должен быть разрешен только для выполнения должностных обязанностей по обслуживанию технических средств системы.

3.10.3. Средства и системы контроля и управления доступом, пожарной безопасности, вентиляции, кондиционирования и видеонаблюдения являются частью инженерной инфраструктуры Заказчика (создается в рамках отдельного проекта) и не входят в состав СЗИ.

3.10.4. СЗИ Системы должны функционировать в штатном режиме при колебании значений параметров окружающей среды (напряжение сети, температура, влажность воздуха и т. п.) в пределах, указанных производителем этих средств.

3.10.5. Специальных требований к защите от влияния внешних воздействий к Системе не предъявляется.

3.11. Требования к патентной чистоте

3.11.1. При проектировании Системы должны соблюдаться положения законодательных актов Российской Федерации по соблюдению авторских прав и защите специальных знаков.

3.11.2. Реализация технических, программных, организационных и иных решений, предусмотренных проектом по созданию Системы, не должна приводить к нарушению авторских и смежных прав третьих лиц.

3.11.3. При проектировании Системы должно использоваться только лицензионное программное обеспечение.

3.11.4. При проектировании в Системе программ (программных комплексов или модулей), разработанных третьими лицами, условия, на которых передается право на использование (исполнение) этих программ, не должны накладывать ограничений, препятствующих использованию Системы по ее прямому назначению.

3.12. Требования по стандартизации и унификации

3.12.1. Все технические решения в рамках проектирования Системы должны основываться на использовании типовых решений и унификации аппаратного обеспечения и ПО.

3.12.2. При проектировании Системы должны выбираться современные технологические решения. При выборе решений приоритет должен отдаваться решениям, которые уже применяются в инфраструктуре Заказчика.

4. Требования к подсистемам СОИБ и их функциям

4.1. Подсистема сбора событий информационной безопасности

4.1.1. Подсистема сбора событий информационной безопасности (далее – Подсистема сбора событий) предназначена для централизованного получения, регистрации, хранения и первичного анализа событий безопасности, возникающих в процессе функционирования объекта критической информационной инфраструктуры (КИИ).

4.1.2. Подсистема сбора событий является компонентом СОИБ и обеспечивает регистрацию событий безопасности для последующего расследования инцидентов (при подтверждении), контроля действий персонала и предоставления данных уполномоченным сотрудникам (администраторам, ответственному за защиту информации).

4.1.3. Подсистема сбора событий должна обеспечивать получение и регистрацию событий от следующих источников, входящих в состав объекта КИИ:

- все компоненты СОИБ (средства антивирусной защиты, межсетевого экранирования, обнаружения вторжений, контроля съемных носителей, анализа защищенности, резервного копирования и т.п.);
- серверное оборудование (включая контроллеры домена, файловые серверы, серверы приложений АСУ);
- автоматизированные рабочие места (АРМ) оперативного и технологического персонала;
- активное сетевое оборудование (коммутаторы, маршрутизаторы), задействованное в технологическом сегменте сети;
- технические средства АСУ (программируемые логические контроллеры, серверы ввода-вывода) — при наличии у них функционала генерации событий и поддержки стандартных протоколов.

4.1.4. Подсистема сбора событий должна выполнять следующие функции:

- получение данных от источников по стандартным протоколам (syslog, SNMP, NetFlow/IPFIX, а также путем чтения текстовых лог-файлов или с использованием легковесных агентов-сборщиков).
- исключение избыточной или незначимой информации на этапе приема для экономии дискового пространства.
- приведение событий из разных источников к единому формату с унификацией временных меток и сворачивание повторяющихся событий в одно с подсчетом количества повторений.
- запись событий в защищенное хранилище с неизменяемостью временных меток и невозможностью модификации записей неуполномоченными лицами.
- предоставление авторизованным пользователям (администраторам, сотрудникам службы безопасности) возможности поиска событий по любым параметрам (время, источник, тип события, пользователь) и просмотра детальной информации.
- создание отчетов по зарегистрированным событиям (например, отчеты по входу в систему, по использованию съемных носителей, по срабатываниям антивируса) за заданный период.
- отправка уведомлений (по электронной почте, через системные сообщения) ответственному лицу при наступлении заданных критических событий (например, многократные ошибки аутентификации, отключение средств защиты).

4.1.5. Подсистема сбора событий должна обеспечивать регистрацию и хранение следующей информации по каждому событию (при наличии в исходном событии):

- дата и время события;
- идентификатор источника события (IP-адрес, имя хоста, имя устройства);
- тип события (код или наименование);
- субъект события (учетная запись пользователя или процесса);
- объект события (имя файла, ресурса, к которому было обращение);
- результат события (успех/неуспех);

- дополнительная информация (текст сообщения, коды ошибок).
- 4.1.6. Требования к надежности хранения
- Информация о событиях безопасности должна храниться в течение срока, установленного политиками Заказчика и законодательством РФ (рекомендуемый срок хранения — не менее 1 года для обеспечения возможности расследования инцидентов).
 - Должна быть обеспечена невозможность удаления или модификации зарегистрированных событий рядовыми пользователями и прикладным программным обеспечением.
 - Выход из строя накопителя, на котором хранятся события, не должен приводить к безвозвратной потере данных. Должна быть предусмотрена возможность резервирования хранилища событий (например, организация RAID-массива или использование отказоустойчивой файловой системы).
- 4.1.7. Требования к интерфейсу и локализации
- Интерфейс администрирования и просмотра событий, а также формируемые отчеты должны быть на русском языке.
 - Должна поддерживаться возможность разграничения прав доступа (ролевая модель): администратор (настройка подсистемы), аудитор (только просмотр и формирование отчетов), оператор (получение уведомлений и ограниченный просмотр).
- 4.1.8. Требования к программному обеспечению
- Программное обеспечение, реализующее функции сбора и хранения событий, должно быть включено в Единый реестр российских программ для ЭВМ и баз данных.
 - Подсистема сбора событий (или ее компоненты) должны быть сертифицированы ФСТЭК России по соответствующим требованиям безопасности информации (применимо к средствам, осуществляющим функции регистрации событий в защищенном исполнении).
- 4.1.9. Подсистема сбора событий должна предоставлять возможность экспорта зарегистрированных событий и данных об инцидентах во внешние системы (при их наличии) в машиночитаемых форматах (CSV, JSON, CEF, XML, LOG, TXT) для последующей передачи в ведомственные центры мониторинга или вышестоящие SIEM-системы. Данное требование не является обязательным для функционирования подсистемы в автономном режиме и реализуется при необходимости, определяемой Заказчиком.

4.2. Подсистема обеспечения однонаправленной передачи данных

4.2.1. Подсистема обеспечения однонаправленной передачи данных (далее - ПФРС) должна представлять собой аппаратно-программный комплекс (диод данных), реализующий гарантированную физическую однонаправленную передачу данных между изолированными сегментами сети.

4.2.2. В составе подсистемы должны применяться сертифицированные средства однонаправленной передачи данных (диоды данных), включенные в реестр российского ПО и имеющие действующий сертификат ФСТЭК России по 4 уровню доверия, что позволяет применять их для защиты объектов критической информационной инфраструктуры (КИИ), в том числе автоматизированных систем управления технологическими процессами (АСУ ТП) до 1 класса включительно.

4.2.3. Архитектура ПФРС должна предусматривать:

- Физический принцип работы, гарантирующий разрыв сети на физическом уровне (отсутствие транзитного соединения, драйверов для обратной передачи, обратной связи по протоколам).
- Возможность организации демилитаризованных зон (DMZ) с размещением серверов-посредников для накопления и последующей передачи данных без возможности обратного доступа в технологическую сеть.
- Наличие универсального API (программного интерфейса) для упрощения встраивания в разнородную инфраструктуру и интеграции с системами-источниками и приемниками данных, включая SCADA, ERP, MES и SIEM-системы

4.2.4. Требования к программной составляющей ПФРС

- Программное обеспечение, входящее в состав ПФРС, должно быть отечественного производства.
- Программное обеспечение должно быть зарегистрировано в едином реестре российских программ для электронных вычислительных машин и баз данных.
- Программное обеспечение должно обладать функциональностью фильтрации и ретрансляции данных на уровне протоколов прикладного уровня, обеспечивая верификацию

передаваемых пакетов в соответствии со спецификациями протоколов.

- Должна обеспечиваться возможность тонкой настройки правил передачи для каждого поддерживаемого протокола (например, разрешенные команды Modbus, диапазоны тэгов OPC UA).
- Программное обеспечение должно обеспечивать формирование детализированных журналов регистрации событий (логов) о переданных данных и срабатываниях правил фильтрации для последующего анализа и отчетности.
- Должны предоставляться интегрированные механизмы оповещения и уведомления администраторов о событиях безопасности и сбоях в работе комплекса.
- Программное обеспечение должно иметь возможность реализации отказоустойчивого кластера для обеспечения высокой доступности (High Availability), гарантируя непрерывность передачи данных и минимальное время простоя при выходе из строя одного из компонентов.
- Должно быть реализовано резервное копирование и восстановление конфигурации комплекса.
- Программное обеспечение должно позволять проводить мониторинг состояния собственных компонентов и диагностики работоспособности каналов связи.
- В программном обеспечении должна быть реализована ролевая модель разграничения доступа к функциям управления и мониторинга.
- ПФРС должна иметь возможность взаимодействовать со смежными системами для синхронизации времени (NTP) и разрешения имен (DNS) в безопасном режиме (только от внешнего контура к внутреннему или наоборот, в зависимости от направления передачи).
- Программный интерфейс (включая средства управления и конфигурирования) должен полностью поддерживать русский язык и использовать кодировку UTF-8.
- Наличие защищенного web-интерфейса (HTTPS) для централизованного управления комплексом и просмотра статусов, полностью русифицированного и поддерживающего современные стандарты безопасности.

4.2.5. Подсистема должна поддерживать передачу следующих типов данных и протоколов:

- Промышленные протоколы: OPC UA/DA, Modbus, IEC-104, MQTT, S7.
- Сетевые протоколы и файловые потоки: UDP (включая Syslog, SNMP traps), FTP(S), CIFS, SFTP, а также возможность передачи RAW TCP трафика.

4.3. Подсистема межсетевого экранирования

4.3.1. Подсистема межсетевого экранирования и предотвращения вторжений (далее – ПМЭ) предназначена для фильтрации сетевого трафика, разграничения доступа между сегментами сети объекта критической информационной инфраструктуры (КИИ), а также для обнаружения и блокирования сетевых атак и вредоносной активности.

4.3.2. ПМЭ должна строиться на базе межсетевых экранов нового поколения (NGFW), обеспечивающих инспекцию трафика на уровнях модели OSI вплоть до прикладного (L7), с обязательной поддержкой анализа промышленных протоколов (Modbus, Profinet, IEC 60870-5-104, OPC DA/UA и др.).

4.3.3. Все компоненты ПМЭ должны соответствовать требованиям ФСТЭК России, предъявляемым к межсетевым экранам согласно приказу ФСТЭК России от 09 февраля 2016 г. № 9 «Об утверждении требований о безопасности информации к межсетевым экранам», и иметь действующие сертификаты ФСТЭК на соответствующие типы исполнения.

4.3.4. Производитель оборудования должен обеспечивать техническую поддержку на территории РФ.

4.3.5. В зависимости от места установки и решаемых задач, состав ПМЭ может включать следующие типы межсетевых экранов (согласно классификации ФСТЭК):

- Тип «А» (Межсетевой экран уровня сети) – применяется на границах технологической сети (например, с сетью вышестоящей организации (системного оператора) или с корпоративным сегментом). Обеспечивает фильтрацию на сетевом и транспортном уровнях, трансляцию адресов (NAT). Реализуется в программно-аппаратном исполнении с производительностью, достаточной для обработки всего трафика на границах без потерь.
- Тип «Д» (Межсетевой экран уровня промышленных сетей) – обязателен к применению для значимых объектов КИИ. Применяется на границе и внутри сегментов для фильтрации промышленных протоколов уровня TCP/IP (например, на верхнем уровне АСУ ТП).

4.3.6. Подсистема должна обеспечивать возможность организации демилитаризованных зон (DMZ) с размещением серверов-посредников (бастионов), не имеющих обратного доступа в технологическую сеть.

4.3.7. ПМЭ должна обеспечивать выполнение следующих функций:

- 1) Фильтрация сетевого трафика
 - Контроль и фильтрация трафика на основе IP-адресов источника и получателя, портов и протоколов транспортного уровня (TCP, UDP, ICMP), с учетом состояния сессий (Stateful Inspection) и по расписанию.
 - Применение правил межсетевого экранирования к фрагментированным, нефрагментированным и любым типам пакетов.
 - Возможность указания в правилах порта источника (не только назначения).
- 2) Контроль приложений и промышленных протоколов (Application Control / DPI L7)
 - Идентификация приложений и сервисов вне зависимости от используемых портов.
 - Для промышленных протоколов (Modbus, Profinet, IEC 60870-5-104, OPC DA/UA и др.) – возможность применения политик, разграничивающих доступ к отдельным функциям (например, разрешить только чтение регистров, запретить запись или выполнение команд).
 - Предоставление интерфейса гибкой настройки правил фильтрации на основе групп доступа пользователей (при наличии интеграции с AD) и сетевых атрибутов.
- 3) Предотвращение вторжений (IPS)
 - Обнаружение и блокирование сетевых атак на основе сигнатурного анализа, поведенческого (эвристического) анализа и анализа аномалий протоколов, включая атаки, специфичные для АСУ ТП.
 - Регулярное обновление баз сигнатур атак (автоматическое или ручное с сайта производителя либо из доверенного репозитория в изолированной сети).
 - Наличие интегрированных механизмов оповещения и уведомления администраторов о событиях безопасности (по электронной почте, через SNMP-трапы, в мессенджеры, в подсистему сбора событий).
- 4) Антивирусная проверка трафика. Блокирование передачи вредоносных файлов в потоковом режиме на протоколах HTTP, FTP, SMTP, POP3, IMAP.
- 5) Контроль веб-трафика (Web Filtering / URL Filtering). Фильтрация доступа к веб-ресурсам по категориям (социальные сети, файлообменники, вредоносные сайты и т.п.) с возможностью создания белых и черных списков.
- 6) Инспектирование зашифрованного трафика (SSL/TLS Inspection). Возможность расшифровки, анализа и повторного шифрования трафика, передаваемого по протоколам SSL/TLS (с использованием TLS-прокси).
- 7) Управление доступом на основе сетевых атрибутов
 - Управление доступом программ и сетевых служб путем разрешения и назначения портов.
 - Возможность создания исключений (режим исключений) для отдельных IP-адресов или подсетей при необходимости проведения регламентных работ.

4.3.8. Требования к управлению и эксплуатации

- 1) Наличие централизованной системы управления, позволяющей:
 - единообразно настраивать политики безопасности на всех компонентах ПМЭ;
 - контролировать состояние и работоспособность всех узлов;
 - осуществлять мониторинг производительности и загрузки в реальном времени;
 - предоставлять инструменты диагностирования состояния собственных компонентов.
- 2) Ролевая модель разграничения доступа:
 - в программном обеспечении должна быть предусмотрена ролевая модель разграничения доступа (администратор безопасности, аудитор, оператор, администратор сети);
 - роли должны иметь ограничения по доступу к функциям управления на уровне интерфейсов, функционала, отчетов и объектов настройки;
 - должно обеспечиваться протоколирование действий администраторов ПМЭ.
- 3) Интерфейс и локализация:

- программный интерфейс компонентов ПМЭ, включая средства управления, а также формы оповещений и уведомлений должен полностью поддерживать русский язык с использованием кодировки UTF-8;

- наличие веб-интерфейса (Web UI) для доступа к компонентам ПМЭ, полностью поддерживающего русский язык.

4) Ведение журналов и отчетность:

- формирование детальных журналов регистрации событий (трафик, срабатывания правил, действия администраторов, системные события);

- возможность экспорта журналов во внешние системы сбора событий (syslog, CEF, JSON) по протоколам UDP/TCP;

- формирование отчетности по заданным шаблонам (в том числе на русском языке).

4.3.9. Требования к надежности и производительности

1) Аппаратные характеристики должны соответствовать требованиям Заказчика по пропускной способности и количеству одновременных сессий с запасом не менее 30% от пиковых нагрузок (с учетом активированных модулей анализа – IPS, DPI, антивирус)

2) Обеспечение высокой доступности:

- поддержка режима отказоустойчивого кластера (Active-Passive или Active-Active) с синхронизацией состояния сессий;

- программное обеспечение должно иметь возможность быть реализованным в соответствии с методом обеспечения высокой доступности, гарантируя минимальное время простоя и полное решение возложенных задач при выходе из строя одного из компонентов;

- возможность вывода части узлов фильтрации из эксплуатации для обслуживания с автоматическим перераспределением нагрузки на оставшиеся узлы прозрачно для пользователей;

- функционал настройки компонентов без остановки всего ПМЭ.

3) Возможность масштабирования производительности путем добавления новых программно-аппаратных компонентов (горизонтальное масштабирование) или улучшения существующих (вертикальное масштабирование).

4) Обеспечение резервного копирования конфигураций компонентов и журналов регистрации событий с возможностью восстановления.

4.3.10. Входящие в состав ПМЭ программные компоненты должны быть российского производства.

4.3.11. Программное обеспечение должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных Минцифры России.

4.3.12. Обновление программного обеспечения и баз сигнатур:

1) наличие механизмов автоматического и ручного обновления программных компонентов (в том числе баз атак, приложений, веб-категорий) с сайта производителя или из доверенного репозитория;

2) возможность настройки периодичности проверки обновлений.

4.4. Подсистема управления доступом

4.4.1. Подсистема управления доступом должна выполнять следующие функции:

управление учетными записями пользователей;

реализация политик управления доступом;

разделение полномочий (ролей) пользователей;

назначение минимально необходимых прав и привилегий;

мониторинг попыток доступа в автоматизированную систему;

блокирование сеанса доступа пользователя при неактивности за исключением станций операторов, которые осуществляют оперативный мониторинг за состоянием технологического процесса; управление действиями пользователей до идентификации и аутентификации.

4.4.2. Для защиты компонентов СОИБ должно применяться специализированное средство защиты информации от НСД. Защиту компонентов ОКИИ необходимо осуществлять компонентами СОИБ и встроенными механизмами ОС.

4.4.3. Специализированное средство защиты информации от НСД должно выполнять следующие функции по защите информации:

контроль входа пользователей в систему и работа пользователей в системе:

- проверка пароля пользователя при входе в систему;

- возможность блокирования входа в систему локальных пользователей;
- возможность блокирования операций вторичного входа в систему в процессе работы пользователей;
- возможность блокировки сеанса работы пользователя по истечении интервала неактивности;
- возможность управления политикой сложности паролей;
- поддержка возможности входа в систему по сертификатам;
- возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей.
- возможность оповещения пользователя о последнем успешном входе в систему;
- возможность выдачи пользователю предупреждения в виде сообщения о том, что в информационной системе реализованы меры защиты информации.

избирательное (дискреционное) управление доступом:

- возможность назначения прав доступа на файлы, каталоги, принтеры, устройства;
- возможность наследования прав доступа для файлов, каталогов и устройств;
- возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту.

полномочное (мандатное) управление доступом:

- возможность заведения в системе не менее 10 уровней конфиденциальности;
- возможность выбора уровня конфиденциальности сессии для пользователя;
- возможность назначения мандатных меток файлам, каталогам, внешним устройствам, сетевым интерфейсам;
- возможность изменения количества мандатных меток в системе и их названий;
- контроль потоков конфиденциальной информации в системе.

контроль аппаратной конфигурации компьютера и подключаемых устройств:

- последовательные и параллельные порты;
- локальные устройства;
- сменные, физические и оптические диски;
- программно-реализованные диски;
- USB-устройства;
- должна быть возможность задать настройки контроля на уровне шины, класса устройства, модели устройства, экземпляра устройства.

• должна быть возможность присвоить устройствам хранения информации мандатную метку. Если метка устройства не соответствует сессии пользователя – работа с устройством хранения должна блокироваться.

• должна быть возможность группового добавления устройств в подсистему контроля устройств без подключения устройства к компьютеру.

регистрация событий безопасности:

- должна быть возможность формирования отчетов по результатам аудита.
- должна быть возможность поиска и фильтрации при работе с данными аудита.

4.4.4. Специализированное средство защиты информации от НСД должно соответствовать требованиям документов: «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности, «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014) не ниже 4 класса защиты, «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ (ФСТЭК России, 2014).

4.5. Подсистема анализа защищенности информации

4.5.1. Подсистема анализа защищенности информации должна выполнять следующие функции:

сетевой аудит в режиме тестирования на проникновение «Pentest»;

идентификация открытых сетевых портов и сервисов;

подбор паролей к СУБД и сетевым службам;

системные аудиты уязвимостей системного и прикладного программного обеспечения;

выявление недостающих обновлений безопасности;

контроль целостности системы;
инвентаризация аппаратного и программного обеспечения сканируемых систем;
формирование отчетов по результатам сканирования.

4.5.2. Реализовывать определение перечня сканируемых узлов на основе ключевого атрибута FQDN (полное доменное имя), IP-адрес элемента ИТ-инфраструктуры:

вводом данных о сканируемых узлах в ручном режиме на основании ключевого атрибута;
интеграцией с единым каталогом домена системы Microsoft Active Directory для импорта списка узлов из базы данных домена с сохранением иерархии контейнеров элементов ИТ-инфраструктуры;
импортом данных из CSV-файла, содержащем ключевые атрибуты.
импортом результатов с обнаруженными узлами сети с помощью сетевого сканирования утилитой Nmap.

4.5.3. Поддерживать и иметь возможность проверки сетевого туннеля в агентном режиме системного сканирования, с использованием специального агентского программного обеспечения, устанавливаемого на сканируемый узел.

4.5.4. Поддерживать и иметь возможность проверки сетевого туннеля в безагентном режиме системного сканирования, с использованием привилегированных учетных записей и соответствующих стандартизованных протоколов WinRM, WMI, SSH, HTTP.

4.5.5. Реализовывать аудит в режиме «Пентест» в рамках сетевого сканирования:

сканирование портов заданной группы сетевых узлов с возможностью выбора режима профиля, диапазона и типов портов TCP или UDP, с результатом идентификации открытых портов и сервисов в графическом окне;

поиск уязвимостей с возможностью выбора точности сканирования;

подбор паролей в виде пары «логин-пароль» для локальных учетных данных к опубликованным сетевым службам Microsoft SQL, PostgreSQL, OracleDB, MySQL, SSH, FTP, POP3 методом полного перебора с возможностью использования внешних словарей, результаты которого должны отображаться в графическом окне.

4.5.6. Результаты сетевого аудита в режиме «Пентест» в рамках поиска уязвимостей должны отображаться в графическом окне и содержать:

идентификатор уязвимости ALTXID, BDU ID, CVE (при наличии);

определение применимости уязвимости CPE;

векторы уязвимости CVSSv2, CVSSv3, CVSSv4, CWE;

уровень риска обнаруженной уязвимости;

описание уязвимости;

рекомендуемые меры по устранению уязвимости, ссылки на БДУ ФСТЭК и ресурсы-источники, в которых содержатся сведения об обнаруженных уязвимостях;

детализация порта и программного обеспечения обнаруженной уязвимости;

уровень точности, используемый при сканировании.

4.5.7. Реализовывать системный аудит уязвимостей системного и прикладного программного обеспечения:

сигнатурный анализ данных, собранных при системном сканировании сетевого узла и предоставлять информацию об обнаруженных уязвимостях;

сканирование группы сетевых узлов;

сканирование платформ, имеющихся у Заказчика.

4.5.8. Должна обладать инструментами по модификации состава и значений параметров профилей аудита и создания собственных конфигураций на основе существующих.

4.5.9. Реализовывать фиксацию и контроль целостности каталогов и файлов по выбранной маске наименования методом контрольного суммирования MD5, SHA1, SHA256, SHA512, ГОСТ Р 34.11-2012.

4.5.10. Реализовывать установку выполненных заданий аудита уязвимостей, инвентаризации и фиксации на контроль для дальнейшего их сравнения с контролируемыми текущими значениями. Результаты должны отображаться в графическом окне Продукта и содержать:

Номер контроля;

Ключевой атрибут сетевого узла;

Статус контроля;

Наименование задания сканирования;

Номер задания сканирования;

Тип задания сканирования;

Дата создания контроля;

Дата завершения задания сканирования;
Детализация соответствия контроля в части добавления, удаления и изменения контролируемых объектов.

4.5.11. Обеспечивать создание заданий по сканированию узлов с параметрами, определяющими время запуска:

- выполнение задания сканирования сразу после создания;
- разовое выполнение задания сканирования в назначенное время;
- выполнение задания сканирования по расписанию с заданной периодичностью.

4.5.12. Должна иметь возможность автоматического создания именований объектов заданий по заданному шаблону.

4.5.13. Подсистема анализа защищенности информации должна реализовывать формирование отчетов по результатам сканирования в форматах PDF, XML, HTML:

- отчет по выбранному диапазону элементов ИТ-инфраструктуры, по последним результатам сканирования;

- отчет по выбранному заданию сканирования;

- дифференциальный отчет, сравнивающий два результата сканирования одной задачи за разные промежутки времени.

4.5.14. Сформированный отчет по результатам сканирования должен содержать следующие разделы:

- статистические данные аудита в виде диаграммы или таблицы;

- сводную информацию о результатах аудита;

- детализированную информацию о данных аудита, сгруппированную по сканируемым элементам ИТ-инфраструктуры.

4.6. Подсистема антивирусной защиты

4.6.1. Подсистема антивирусной защиты должна включать в себя:

Подсистему комплексной защиты конечных узлов. Данная подсистема должна быть применима для АРМ, базы данных, сервера и т.п. (в том числе для устройств верхнего уровня АСУ)

Подсистему централизованного администрирования. Данная подсистема должна обеспечивать централизованное управление параметрами подсистемы защиты конечных узлов, а также осуществлять сбор информации о событиях информационной безопасности от подсистемы защиты конечных узлов и подсистемы мониторинга технологической сети.

4.6.2. Подсистема антивирусной защиты должна обеспечивать возможность оперативного оповещения персонала о выявленных событиях и инцидентах ИБ.

4.6.3. Подсистема защиты конечных узлов должна обеспечивать комплексную защиту узлов промышленных устройств системы управления и обладать следующей функциональностью:

- постоянная защита конечных узлов от заражения вредоносным программным обеспечением;
- периодическая проверка конечных узлов на наличие вредоносного программного обеспечения;
- контроль запуска приложений (белый список) в блокирующем и неблокирующем режимах;
- контроль подключения внешних устройств (USB-носители, CD-приводы, мобильные устройства

МТР, модемы) в блокирующем и неблокирующем режимах;

- контроль подключений к беспроводным сетям;

- управление настройками межсетевого экрана ОС Windows;

- защита от шифрования файлов на общих сетевых ресурсах;

- контроль изменений произвольных файлов на диске;

- анализ журналов операционной системы;

- защита от эксплойтов;

- централизованное управление и распространение обновлений антивирусных баз;

- регистрация инцидентов.

4.6.4. ПО подсистемы защиты конечных узлов должно быть совместимо со следующими ОС:

Windows (7, 8, 10, 11); Windows Server (2012, 2016, 2019, 2022);

Astra Linux, ALT Linux, Ред ОС, Ubuntu, CentOS, Debian и т.п.

4.6.5. ПО подсистемы должно быть совместимо с ПО, обеспечивающим и поддерживающим выполнение технологического процесса (ПО SCADA, инженерные системы конфигурирования и разработки).

4.6.6. Подсистема централизованного администрирования должна обеспечивать возможность удалённого конфигурирования подсистемы защиты конечных узлов посредством единообразного пользовательского интерфейса, а также должна обеспечивать долговременное хранение и отображение поступающих оповещений от подсистемы мониторинга технологической сети и подсистемы защиты конечных узлов.

4.6.7. Подсистема централизованного администрирования должна обладать следующей функциональностью:

- централизованное назначение политик безопасности подключённым узлам промышленной сети;
- управление обновлениями программного обеспечения;
- долговременное хранение оповещений о выявленных событиях и инцидентах ИБ в защищённой базе данных;
- отображение журнала оповещений о выявленных событиях и инцидентах ИБ в удобной пользователю форме;
- построение консолидированных отчётов о статусе кибербезопасности;
- реализация оперативного оповещения обслуживающего персонала;
- отображение статуса защищённости технологической сети;
- возможность удалённого администрирования сервера с нескольких рабочих мест (с настраиваемым разграничением прав пользователей).

4.7. Подсистема резервного копирования

4.7.1. ПО подсистемы резервного копирования должна соответствовать следующим системным требованиям:

4.7.2. ПО должно иметь возможность резервного копирования, шифрования резервных копий и аварийного восстановления данных на компьютерах, работающих под управлением следующих ОС:

Windows (7, 8, 10, 11); Windows Server (2012, 2016, 2019, 2022);

Astra Linux, ALT Linux, Ред ОС, Ubuntu, CentOS, Debian и т.п.

ПО должно поддерживать следующие способы загрузки:

BIOS;

UEFI.

ПО должно поддерживать следующие файловые системы:

FAT16/32;

NTFS.

ПО должно поддерживать следующие носители информации:

жесткие диски HDD и SSD;

сетевые устройства хранения (SAN и NAS);

RAID-массивы;

P-ATA (IDE), S-ATA, SCSI, IEEE1394 (Firewire) и накопители USB 1.1 / 2.0 / 3.0, устройства хранения данных PCMCIA;

сервер SFTP;

ленточные устройства, автоматические загрузчики и библиотеки, а также управление носителями и поддержка баркодов.

4.7.3. ПО должно обеспечивать следующие основные функции и возможности:

ПО должно обеспечивать резервное копирование и аварийное восстановление дисков и томов со всеми хранящимися на них данными (включая приложения).

Сервер управления ПО должен устанавливаться на ОС Windows.

В ПО должен присутствовать WEB интерфейс управления сервером.

ПО должно обеспечивать резервное копирование и аварийное восстановление папок и файлов.

4.7.4. ПО должно поддерживать следующие функции и возможности резервного копирования:

создание полных, дифференциальных и инкрементных резервных копий;

слияние инкрементных и дифференциальных резервных копий;

автоматическое удаление устаревших резервных копий;

сжатие;

исключение файлов;

автоматическое или ручное разбиение резервных копий;

дедупликация.

4.7.5. ПО должно поддерживать следующие функции и возможности восстановления из резервных копий:

- восстановление при загрузке;
- восстановление на «голое железо»;
- восстановление файлов, сохраняя настройки безопасности;
- возможность изменить SID пользователя при восстановлении;
- копирование отдельных файлов или папок из резервной копии с помощью Windows Explorer.

4.7.6. ПО должно поддерживать следующие функции и возможности управления резервными копиями:

- шаблоны схем резервного копирования;
- Команды до и после резервного копирования;
- настраиваемая схема резервного копирования;
- защита резервной копии с помощью пароля/шифрования;
- условия удаления резервных копий – количество копий, возраст копии;
- создание резервной копии вместе с загрузочными компонентами на съемный загрузочный носитель для возможности аварийного восстановления.

4.7.7. ПО должно ограничивать доступ к управлению резервным копированием и восстановлением данных для пользователя и групп пользователей путём авторизации.

4.7.8. Должен поддерживаться запуск заданий на создание резервной копии согласно заданному расписанию.

4.7.9. ПО должно позволять создавать загрузочные носители на основе ОС Linux и WinPE.

4.7.10. ПО должно поддерживать следующие дополнительные функции:

восстановление образов серверов на «голое» железо и на оборудование, отличное от того, с которого были сняты резервные копии;

защита от вирусов-шифровальщиков;

возможность перед стартом задачи на резервирование, проверки состояния служб Microsoft VSS и устранение проблем с ними;

4.7.11. Подписка на техническую поддержку ПО должна предоставлять следующие возможности:

- Контакт со службой технической поддержки посредством телефона, электронной почты.
- Техническая поддержка должна быть доступна на русском языке в рабочие часы, в будни.
- Обозначение критичности проблемы при создании заявке в службе технической поддержке.
- В критичных случаях при обращении в службу технической поддержки первая реакция инженера должна последовать в течение нескольких часов.
- Подписка на техническую поддержку в период своего действия должна гарантировать бесплатные обновления продукта, в том числе переход на новую версию продукта.

4.7.12. ПО должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных.

5. Требования к видам обеспечения

5.1. Требования к информационному обеспечению

5.1.1. Уровень совместимости и состав данных при взаимодействии со смежными системами должны быть определены на стадии разработки технического проекта.

5.1.2. При взаимодействии со смежными системами должны использоваться стандартизированные сетевые протоколы и форматы данных, поддерживаемые данными системами.

5.1.3. Должно использоваться средство управления базами данных широко известных производителей, или оно должно быть встроено в СЗИ Системы.

5.1.4. Данные в Системе должны быть защищены от аварий и сбоя электропитания посредством применения источников бесперебойного питания для поддержания функционирования и регулярного резервного копирования данных встроенными механизмами СЗИ Системы или с применением сторонних средств резервного копирования.

5.1.5. В Системе должно вестись протоколирование функционирования, достаточное для выяснения причины аварии (сбоя).

5.2. Требования к программному обеспечению

5.2.1. ПО должно представлять собой совокупность системного и прикладного ПО, реализующего совместно с ТС цели и задачи Системы.

5.2.2. При проектировании Системы должны использоваться коммерческие программные продукты и (или) встроенные в прикладное или системное ПО механизмы ИБ.

5.2.3. Решения по использованию ПО должны приниматься с учетом обеспечения поддержки его функционирования производителем или поставщиком данного ПО.

5.3. Требования к техническому обеспечению

5.3.1. Аппаратные компоненты Системы должны базироваться на аппаратных платформах, обеспечивающих функции диагностики, резервирования и взаимозаменяемости.

5.3.2. Для серверных компонентов Системы должны быть предусмотрены решения, обеспечивающие возможность наращивания производительности и объема хранимой информации.

5.3.3. Состав технических средств СЗИ должен выбираться, исходя из требований их совместимости и функциональной полноты для реализации поставленных задач при минимально необходимой номенклатуре.

5.4. Требования к организационному обеспечению

5.4.1. В рамках работ по проектированию Системы должны быть определены: рекомендации к структуре и функциям подразделений, участвующих в функционировании Системы или обеспечивающих ее эксплуатацию;

рекомендации по количеству, структуре и квалификации персонала, осуществляющего обслуживание Системы;

рекомендации к организации функционирования Системы.

5.4.2. Организационная структура должна обеспечивать:

организацию работы по защите информации ОКИИ;

развитие и контроль выполнения требований нормативно-методической базы защиты информации;

администрирование и эксплуатацию Системы.

5.4.3. Указанные рекомендации должны быть приведены и описаны в Пояснительной записке на создание Системы.

6. Состав и содержание работ по созданию системы

6.1. Работы в объёме настоящего Технического задания должны включать в себя:
 обследование объекта защиты;
 разработка модели угроз и нарушителя;
 формирование требований к Системе;
 техническое проектирование;
 разработка рабочей документации;
 разработка эксплуатационной документации;
 разработка организационно-распорядительной документации;
 согласование с ФСТЭК России разработанной документации (в случаях, предусмотренных законодательством РФ для 1-2 категории значимости);
 анализ действующей системы и существующих организационно-технических мер;
 подготовка методики испытаний СОИБ.

6.2. Перечень документов, предъявляемых по окончании соответствующих этапов работ:

Этап	Отчетные документы и работы
Обследование объекта защиты	Предпроектное обследование, заполненные опросные листы, отчет об обследовании.
Разработка моделей угроз и нарушителя	Модели угроз и нарушителя безопасности информации
Техническое проектирование	Ведомость технического проекта Пояснительная записка к техническому проекту Схема структурная Схема функциональная Схема логическая
Разработка рабочей документации	Спецификация оборудования и программного обеспечения Системы; Схема соединений внешних проводов; Таблица соединений и подключений; Чертеж установки технических средств; План расположения оборудования и проводов; Программа и методики испытаний.
Разработка эксплуатационной документации	Ведомость эксплуатационных документов; Руководство администратора Системы; Руководство пользователя Системы; План резервного копирования.
Формирование требований к Системе	Техническое задание на внедрение Системы

6.3. Состав организационно-распорядительной документации:

№ п/п	Наименование документа	Основание для разработки документа	Ограничения
1	Регламент идентификации и аутентификации (ИАФ)	ИАФ.0 приказа ФСТЭК №239	
2	Регламент управления доступом (УПД)	УПД.0 приказа ФСТЭК №239	Документ не должен содержать матриц доступа
3	Регламент защиты машинных носителей информации (ЗНИ)	ЗНИ.0 приказа ФСТЭК №239	
4	Регламент аудита информационной безопасности	АУД.0 приказа ФСТЭК №239	Документ должен содержать требования к проведению

№ п/п	Наименование документа	Основание для разработки документа	Ограничения
	(АУД)	п. 36 приказа ФСТЭК №235	аудитов. Документ не должен содержать программ аудитов, планов проведения аудитов
5	Регламент антивирусной защиты (АВЗ)	АВЗ.0 приказа ФСТЭК №239	
6	Регламент обеспечения целостности (ОЦЛ)	ОЦЛ.0 приказа ФСТЭК №239	
7	Регламент обеспечения доступности (ОДТ)	ОДТ.0 приказа ФСТЭК №239	
8	Регламент защиты технических средств и систем (ЗТС)	ЗТС.0 приказа ФСТЭК №239	
9	Регламент защиты информационной (автоматизированной) системы и ее компонентов (ЗИС)	ЗИС.0 приказа ФСТЭК №239	
10	Регламент реагирования на компьютерные инциденты (ИНЦ)	ИНЦ.0 приказа ФСТЭК №239 пп. б) п.25 приказа ФСТЭК №235 пп. в) п.25 приказа ФСТЭК №235	Документ не должен содержать карточек событий и инцидентов, форм отчета о событии и отчета об инциденте. Документ должен содержать требования к реагированию на инциденты, конкретные инструкции по реагированию не должны разрабатываться
11	Регламент управления конфигурацией информационной (автоматизированной) системы (УКФ)	УКФ.0 приказа ФСТЭК №239	Документ должен содержать требования к управлению конфигурацией. Документ не должен содержать конкретных конфигураций систем.
12	Регламент управления обновлениями программного обеспечения (ОПО)	ОПО.0 приказа ФСТЭК №239	
13	Регламент планирования мероприятий по обеспечению защиты информации (ПЛН)	ПЛН.0 приказа ФСТЭК №239	
14	Регламент обеспечения действий в нештатных ситуациях (ДНС)	ДНС.0 приказа ФСТЭК №239	
15	Регламент информирования и обучения персонала (ИПО)	ИПО.0 приказа ФСТЭК №239	Документ не должен содержать планов обучения, программ обучения
16	Проект приказа «О создании системы безопасности объектов КИИ (и внедрении организационных мер по обеспечению безопасности Объекта защиты)»	п. 9 Приказа ФСТЭК № 235	Должен быть подготовлен шаблон. Конкретные должности и ФИО заполняются Заказчиком.
17	Регламент оценки соответствия средств защиты информации по требованиям информационной безопасности	п. 18 приказа ФСТЭК № 235 пп. б) п. 25 приказа ФСТЭК № 235 п. 28 приказа ФСТЭК № 239	Документ должен содержать требования к проведению оценки соответствия. Документ не должен

№ п/п	Наименование документа	Основание для разработки документа	Ограничения
			содержать Программу и методики испытаний конкретных технических средств и систем.
18	Положение об обеспечении безопасности ЗОКИИ	пп. а); б); в) п. 25 приказа ФСТЭК № 235 п. 33 Приказа ФСТЭК № 235 пп. в) п. 13.1 приказа ФСТЭК № 239	
19	Проект приказа о создании комиссии по контролю состояния обеспечения безопасности КИИ	п. 36 приказа ФСТЭК № 235	Должен быть подготовлен шаблон. Конкретные должности и ФИО Заказчиком.
20	Проект приказа об установлении контролируемой зоны	ЗТС.2 приказа ФСТЭК № 239	Должен быть подготовлен шаблон. Конкретные должности и ФИО заполняются Заказчиком.
21	План действий в нештатных ситуациях	ДНС.1 приказа ФСТЭК № 239 п. 12.2 приказа ФСТЭК № 239 пп. а) п. 13.6 приказа ФСТЭК № 239	
22	Проект приказа о распределении ответственности в области обеспечения безопасности Объекта защиты	п. 10 приказа ФСТЭК № 235 пп. г) п. 12.3 приказа ФСТЭК № 239	Должен быть подготовлен шаблон. Конкретные должности и ФИО заполняются Заказчиком.
23	Должностные инструкции лиц, ответственных за обеспечение безопасности Объекта защиты	п. 13 приказа ФСТЭК № 235	Должно быть подготовлено не более 2 должностных инструкций.
24	Положение о подразделении, ответственном за обеспечение безопасности Объекта защиты	п.10, п.12, п.14 Приказа ФСТЭК № 235	
25	Ежегодный план мероприятий по обеспечению безопасности ЗОКИИ (отдельные планы мероприятий в подразделениях)	п. 13.1 приказа ФСТЭК № 239 пп. б) п.25 приказа ФСТЭК № 235 п. 29 приказа ФСТЭК № 235	Календарные сроки выполнения мероприятий устанавливаются Заказчиком. В документе должны быть указаны требования или рекомендации к таким срокам.
26	Журнал ознакомления с ОРД по КИИ или листы ознакомления с отдельными документами	п. 15 приказа ФСТЭК № 235 п. 27 приказа ФСТЭК № 235	Должен быть подготовлен шаблон. Заполняется Заказчиком.
27	Журнал ознакомления подрядчиков с ОРД по КИИ	п. 16 приказа ФСТЭК № 235	Должен быть подготовлен шаблон. Заполняется Заказчиком.
28	Правила безопасности при эксплуатации Объекта защиты	п. 12.2 приказа ФСТЭК № 239 п. 15 приказа ФСТЭК № 235 пп. в) п.25 приказа ФСТЭК № 235	
29	Акт оценки эффективности принятых организационных и	п.36 Приказа ФСТЭК № 235	Должен быть подготовлен шаблон. Заполняется

№ п/п	Наименование документа	Основание для разработки документа	Ограничения
	технических мер по обеспечению безопасности Объекта защиты		Заказчиком.
30	Инструкция о порядке учета, хранения, обращения и уничтожения машинных носителей информации	ЗНИ.1 приказа ФСТЭК № 239	
31	Журнал учета машинных носителей информации	ЗНИ.1 приказа ФСТЭК № 239 п. 2, ст. 19	Должен быть подготовлен шаблон. Заполняется Заказчиком.
32	Журнал проведения инструктажей по информационной безопасности и обеспечению безопасности КИИ	п. 15 приказа ФСТЭК № 235	Должен быть подготовлен шаблон. Заполняется Заказчиком.
33	Проект приказа об утверждении комплекта документов по обеспечению безопасности КИИ	п.23 Приказа ФСТЭК № 235	Должен быть подготовлен шаблон. Конкретные должности и ФИО заполняются Заказчиком.
34	Регламент взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)	пп. б) п. 25 приказа ФСТЭК №235; требования ФСБ России в области обнаружения, предупреждения и ликвидации последствий компьютерных атак (в соответствии с приказами ФСБ России, вступившими в силу с 30.01.2026, регламентирующими непрерывное взаимодействие с НКЦКИ и порядок информирования об инцидентах и компьютерных атаках)	Документ не должен содержать карточек событий и инцидентов. Должен учитывать сокращенные сроки реагирования (3 часа для ЗОКИИ)

Состав организационно-распорядительной документации может измениться после проведения обследования по согласованию с отделом безопасности КИИ АО «ЭН+ ГЕНЕРАЦИЯ».

7. Порядок контроля и приемки работ

- 7.1. Критериями для приемки работ являются требования настоящего Технического задания.
- 7.2. Приемка и сдача выполненных работ осуществляются совместной комиссией, назначаемой приказом или внутренним распоряжением Заказчика в соответствии с этапностью создания Системы.
- 7.3. Этапы закрываются актами о выполнении соответствующих работ.
- 7.4. Настоящее Техническое задание может быть уточнено или изменено в процессе разработки. Уточнения и изменения производятся по согласованию с отделом безопасности КИИ АО «ЭН+ ГЕНЕРАЦИЯ» и Заказчиком. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего Технического задания.
- 7.5. Согласование и утверждение изменений производятся в том же порядке, что и согласование, и утверждение настоящего Технического задания.

8. Требования к Исполнителю

- 8.1. Исполнитель должен иметь действующую лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.
- 8.2. Исполнитель должен иметь опыт работы на рынке услуг в области информационной безопасности не менее 5 лет.
- 8.3. Участник должен соответствовать требованиям менеджмента качества ISO 9001:2015.

Требования к проектной и рабочей документации

1. Этапы создания документации

1.1. 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 совместно с Заказчиком. Заказчик обеспечивает доступ на объект и оказывает необходимое содействие в сборе исходных данных;
- результаты предпроектного обследования согласуются с Заказчиком, департаментом по эксплуатации «ЭН+ ГИДРО».

1.2. 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, разработанный с учетом требований Приказа АО «ЭН+ ГЕНЕРАЦИЯ» от 24.06.2026 №ГЕН-П-26-183 «Об утверждении состава системы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры».

В техническом задании должны быть детализированы и согласованы все технические решения, необходимые для технического перевооружения САУ ГА, сетевого оборудования и оборудования верхнего уровня. 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.

1.3. Разработка ОТР и ТТ на поставку оборудования

На основании данных, полученных при проведении предпроектного обследования необходимо разработать и согласовать с заказчиком основные технические решения, а также технические требования, опросные листы для проведения конкурсных процедур на оборудование системы автоматического управления гидроагрегатов (САУ ГА) ООО «ЭН+ ГИДРО КАРЕЛИЯ», модернизация и поставка которого требуется для выполнения работ и места его расстановки.

1.4. Разработка ПД и РД

Разработать проектную и рабочую документацию на основе исходных данных, представленных Заказчиком и предпроектного обследования «Системы автоматического управления гидроагрегатов (САУ ГА) ООО «ЭН+ ГИДРО КАРЕЛИЯ»». Согласовать с Заказчиком и департаментом по эксплуатации «ЭН+ ГИДРО».

1.5. Разработка ПСД

Необходимо разработать и согласовать с заказчиком проектно-сметную документацию на техническое перевооружение «Системы автоматического управления гидроагрегатов (САУ ГА) ООО «ЭН+ ГИДРО КАРЕЛИЯ». Разработка проектной, рабочей и сметной документации может выполняться параллельно.

2. Объем проектной и рабочей документации

2.1. 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»;
- Постановление Правительства Российской Федерации от 08.02.2018 № 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»

- 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 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»;
- Приказ АО «ЭН+ ГЕНЕРАЦИЯ» от 24.06.2026 №ГЕН-П-26-183 «Об утверждении состава системы обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры»;
- СТП ЭНГ.202.115-2026 «Ценообразование в ремонтной, строительной деятельности, услуг производственного и непроизводственного (технического) характера» ООО «ЭН+ ГИДРО».

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

2.2. 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;
- пояснительная записка к эскизному проекту;
- пояснительная записка к техническому проекту;
- ведомость технического проекта;
- ведомость покупных изделий;
- графические логические схемы и блок-схемы алгоритмов технологических процессов;
- логические схемы локальной вычислительной сети САУ ГА;
- протоколы сетевых сервисов, отражающих информационный обмен между компонентами системы;
- протоколы сетевых сервисов, отражающих информационный обмен с внешними автоматизированными системами;
- перечень входных сигналов (физических, цифровых; аналоговых, дискретных);
- перечень выходных сигналов (физических, цифровых; аналоговых, дискретных);
- описание автоматизируемых функций;
- описание информационного обеспечения системы;
- описание организации информационной базы;
- описание систем классификации и кодирования;
- описание массива информации;
- описание комплекса технических средств;
- описание программного обеспечения;
- описание организационной структуры;
- ведомость оборудования и материалов;

- локальный сметный расчет.

Проектная документация на САУ ГА должна быть разработана как типовая, с возможностью ее использования при дальнейшей поэтапной реконструкции систем управления и сигнализации гидроагрегатов «ЭН+ ГИДРО КАРЕЛИЯ».

2.3. Рабочая документация должна включать в себя:

- ведомость документов;
- спецификации оборудования, изделий и материалов, комплектующих и ЗИП;
- схема структурная комплекса технических средств;
- описание информационного массива;
- описание базы данных;
- схема принципиальная;
- схема соединения внешних проводок;
- схема подключения внешних проводок;
- таблица соединений и подключений;
- чертежи общего вида;
- чертежи установки технических средств;
- физические схемы локальной вычислительной сети САУ ГА;
- программы и методики испытаний компонентов, подсистем, систем, комплексов автоматизации;
- 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;
- локальная смета;
- задание заводу на изготовление шкафов;
- описание технологического процесса обработки данных (включая телеобработку);
- общее описание системы;
- задание на разработку прикладного программного обеспечения (ППО);
- руководство администратора;
- руководство пользователя;
- руководство программиста;
- инструкция по эксплуатации комплекса технических средств;
- физическую и логическую схемы с подробной привязкой к объекту.

2.4. 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.

2.5. Разработку прикладного программного и информационного обеспечений, на стадии «Рабочая документация» не выполнять. Затраты на разработку предусмотреть в сметной документации для выполнения на этапе пуско-наладочных работ.