



УТВЕРЖДАЮ

Заместитель директора по производству
- главный инженер
ООО «ЭН+ГИДРО»

Ю.В. Дворянский
« ____ » _____ 2026 г.

ЗАДАНИЕ

**на разработку документации по информационной безопасности по объекту
"ОРУ 220-500 кВ. УИГ_00040406. Техническое перевооружение АДВ Усть-Илим-
ской ГЭС"**

1. Основания для проведения работ

План капитальных вложений на капитальное строительство на 2026 год, утвержденный директором ООО «ЭН+ ГИДРО».

2. Вид строительства

Техническое перевооружение.

3. Район и площадка строительства

Иркутская область, г. Усть-Илимск, территория филиала ООО «ЭН+ ГИДРО»
Усть-Илимская ГЭС.

4. Нормативно-технические документы, определяющие требования к оформлению и содержанию проекта

- Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСТЭК России от 21 декабря 2017 г. №235 «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказ ФСТЭК России от 25 декабря 2017 г. №239. «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСТЭК России от 14 марта 2014 г. №31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;
- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении»;
- Стандарт «Управление информационной безопасностью критической информационной инфраструктуры технологического сегмента», утв. приказом АО «ЭН+ ГЕНЕРАЦИЯ» от 23.04.2025 № ГЕН-П-25-076;

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

5. Требования к разрабатываемой документации

5.1. Разрабатываемая документация должна являться частью томов (отдельным разделом) рабочей документации по титулу "ОРУ 220-500 кВ. УИГ_00040406.

Техническое перевооружение АДВ Усть-Илимской ГЭС" и включать в себя все требования по информационной безопасности для проектируемого объекта на основании требований нормативных документов и принятой категории значимости (класса защищенности).

5.2. При проектировании необходимо выполнить:

- разработку технических средств защиты информации проектируемой АДВ при приеме (передаче) данных по каналам связи с диспетчерскими центрами – Филиалом АО «СО ЕЭС» Иркутское РДУ, Филиалом АО «СО ЕЭС» ОДУ Сибири; со смежными объектами электроэнергетики; с внешними информационными сетями через существующий диод данных. При разработке данных решений учитывать проект «Обеспечение кибербезопасности в ТИВС с УВ по Усть-Илимской ГЭС» и типовую схему организации информационно-вычислительных сетей (приложение 1);
- разработать организационные требования к защите информации в соответствии с действующими нормативными документами;
- разработать необходимый комплект эксплуатационной документации по защите информации.

5.3. При проектировании необходимо провести категорирование объекта и присвоение одной из категории значимости в соответствии с учетом Постановлением Правительства РФ 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».

5.4. Разрабатываемая документация должна содержать, но не ограничиваться:

- детализированное техническое задание;
- общая пояснительная записка;
- технические требования к построению системы защиты;
- технический проект на создание системы защиты;
- спецификации оборудования и ПО;
- программа пусконаладочных работ (ППНР);
- программа и методика испытаний (ПМИ);
- комплект организационно-распорядительной документации.

5.5. Модель угроз необходимо разработать в соответствии с методическим документом ФСТЭК «Методика оценки угроз безопасности информации» от 05.02.2021 г.

5.6. Набор мер по обеспечению информационной безопасности должен быть адаптирован на основании разработанной модели угроз.

5.7. Набор мер должен обеспечивать нейтрализацию всех актуальных угроз безопасности информации и соответствовать организационно-техническим мерам, предусмотренным в Приказах ФСТЭК №31 от 14.03.2014 г., № 239 от 25.12.2017 г., №159 от 28.08.2024 г. в зависимости от присвоения категории значимости.

5.8. Планируемые к реализации мероприятия по информационной безопасности не должны оказывать негативного влияния на работу проектируемого оборудования АДВ.

5.9. Проектируемые средства защиты информации должны иметь действующие сертификаты ФСТЭК России и/или ФСБ России.

5.10. Все проектируемые средства защиты информации должны быть обеспечены гарантийной и (или) технической поддержкой на весь период эксплуатации.

5.11. Должно быть предусмотрено горячее резервирование проектируемого оборудования, непосредственно участвующего в обработке технологической информации.

5.12. Все проектируемые средства защиты информации (входящие в их состав 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).

5.13. Программное обеспечение, используемое в составе программно-аппаратных комплексов (и/или программно-аппаратных средств) проектируемых средств защиты, должно быть включено в единый реестр российских программ для электронных вычислительных машин и баз данных.

5.14. Взаимодействие технологических сетей АДВ с сетью Интернет не допускается.

5.15. Взаимодействие технологических сетей АДВ с внешними выделенными сетями должно быть организовано через межсетевой экран с организацией ДМЗ зон (сегмента сети без управляющего воздействия, используя промежуточные сервера).

5.16. Взаимодействие между сетями и сегментами внутри технологических сетей АДВ должно осуществляться исключительно через физические интерфейсы, организованные на межсетевом экране.

5.17. Сегментирование должно быть проведено таким образом, чтобы исключить возможность доступа между сегментами в обход межсетевого экрана.

5.18. Планируемые к реализации мероприятия по информационной безопасности должны включать комплекс технических, организационных и программно-алгоритмических мер.

5.19. Организационные меры должны предусматривать размещение аппаратуры в помещениях, защищенных от доступа лиц, не имеющих допуска к работе с оборудованием АДВ. При размещении аппаратуры в незащищенных помещениях аппаратура конструктивно должна быть скомпонована в шкафах, защищенных от доступа посторонних лиц.

5.20. Программно-алгоритмические меры должны обеспечивать персоналу различных категорий доступ к выполнению функций и задач по изменению настроечных параметров АДВ и технических средств в соответствии с его правами, определяемыми именем и паролем.

5.21. Пользователям АРМ и серверов необходимо присваивать минимально необходимые права и полномочия доступа для выполнения своих должностных обязанностей.

5.22. Для предотвращения несанкционированного доступа к информации должна быть предусмотрена возможность установки программных паролей.

5.23. Должны быть предусмотрены функции антивирусной защиты серверов, АРМ, включающие в себя:

- защиту от внедрения (заражения) вредоносными компьютерными программами (вирусами);
- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации) при загрузке, открытии или исполнении таких файлов;
- проведение периодических проверок компонентов объекта защиты на наличие вредоносных компьютерных программ (вирусов);
- оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);
- контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации;
- контроль подключения съемных машинных носителей информации;
- контроль целостности программного обеспечения.

5.24. Использование съемных носителей информации пользователями в период штатной эксплуатации допускается только администратором для целей обновления

ПО и архивирования системных и технологических журналов, а также рабочих наборов данных. Перед использованием сменные носители информации в обязательном порядке должны проверяться средствами защиты от вредоносного ПО с актуальными базами сигнатур.

5.25. Организационные меры должны обеспечивать выполнение работ по эксплуатации и обслуживанию оборудования персоналом различных категорий только в пределах своей компетенции, оговоренной должностными инструкциями и эксплуатационной документацией. Все работы по вскрытию и ремонту аппаратуры, переустановке ПО должны выполняться с оформлением допуска в установленном порядке.

5.26. ТЛВС и каналы связи должны быть защищены:

- от физического подключения;
- от несанкционированной передачи трафика;
- порты должны иметь защиту от подключения по MAC-адресу;
- свободные порты должны быть заблокированы.

5.27. Все порты и сервисы межсетевых экранов и внешних потребителей информации должны быть закрыты по умолчанию. При этом открываются лишь те, которые необходимы для функционирования АДВ. Межсетевые экраны должны быть настроены по принципу запрета прохождения любого трафика кроме минимально необходимого для работы (принцип «белого списка»).

5.28. Доступ из общестанционной сети в технологическую ЛВС АДВ должен быть исключен. Не допускается подключение любого устройства через технологии беспроводной связи.

5.29. В технологической ЛВС АДВ должны быть запрещены:

- удаленный доступ к устройствам и программно-техническим средствам для технического сопровождения системного и прикладного ПО, за исключением удаленного доступа к серверам, расположенным в зоне ДМЗ, и за исключением доступа со специализированных АРМ, входящих в состав АДВ;
- доступ к ресурсам АДВ из информационно-вычислительной сети общего пользования Интернет, сервисы доступа в сеть Интернет и электронный почты.

5.30. С целью обеспечения поддержания актуального состояния системы безопасности необходимо организовать обновление ОС, СУБД, антивирусного ПО, прикладного ПО иного оборудования. Указания по обновлению ОС, СУБД и ПО необходимо отразить в разрабатываемой документации.

5.31. Должны быть реализованы следующие организационные и технические меры защиты:

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

- информирование и обучение персонала (ИПО).

Набор мер по обеспечению безопасности может быть адаптирован и дополнен. Набор мер должен быть минимально достаточным для обеспечения безопасности значимого объекта КИИ 3 категории значимости.

5.32. Комплект организационно-распорядительной документации по защите информации должен включать документы (но не ограничиваться) и покрывать все требования по документированию процессов информационной безопасности, установленные приказами ФСТЭК России (№235, №239, №159):

- политику антивирусной защиты;
- политику резервного копирования;
- политику осведомленности и обучения персонала в области ИБ;
- политику обеспечения действий в нештатных ситуациях;
- регламент управления доступом;
- регламент обеспечения сетевой безопасности;
- регламент обеспечения целостности;
- регламент проведения аудитов безопасности;
- регламент управления инцидентами ИБ;
- регламент обеспечения непрерывности;
- регламент управления обновлениями и уязвимостями;
- регламент управления изменениями;
- инструкцию по защите машинных носителей;
- инструкцию по обеспечению физической защищенности компонентов информационной системы;
- правила поведения пользователей в информационной системе;
- положение о подразделении, ответственном за обеспечение безопасности КИИ;
- порядок контроля выполнения мероприятий по обеспечению безопасности КИИ;
- порядок взаимодействия с ГосСОПКА.

5.33. Состав проектной документации может быть дополнен по предложению Исполнителя.

5.34. В составе документации должна быть разработана программа пусконаладочных работ по проверке разработанных проектных решений после их реализации. К программе должны быть приложены сведения необходимые для разработки сметной документации на пусконаладочные работы.

6. Особые условия проектирования

Действующее предприятие.

7. Требования к исполнителю

Исполнитель должен иметь квалифицированный персонал, обладающий дипломами и сертификатами, подтверждающими его квалификацию по направлению «информационная безопасность» и в области обеспечения безопасности технологических систем.

Наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации (работы и услуги по проектированию в защищенном исполнении средств и систем информатизации).

8. Дополнительные требования

В процессе разработки документации она должна быть согласована с разработчиком основных разделов по проекту - ООО «Прософт-Системы», а также Исполнителем должно быть проверено, что разработанные им решения реализованы ООО

«Прософт-Системы» в смежных (связанных) томах рабочей документации по объекту "ОРУ 220-500 кВ. УИГ_00040406. Техническое перевооружение АДВ Усть-Илимской ГЭС". Все выявленные отклонения должны быть оформлены в официальной переписке.

Разработанная документация и проектируемые средства защиты информации должны быть согласованы с Заказчиком, управлением ООО «ЭН+ ГИДРО», отделом безопасности КИИ АО «ЭН+ ГЕНЕРАЦИЯ» и с УИБ «ДЗР Сибирь».

Документация предоставляется в бумажном и электронном виде в формате:

- вся документация обязательно предоставляется в редактируемом формате (файлы DWG-AutoCad и VSD-Visio, DOC-Word, XLS-Excel) на электронном носителе (в одном экземпляре);

- вся документация обязательно предоставляется в отсканированном виде с подписями в файлах PDF на электронном носителе (в одном экземпляре);

- подписанная документация (оригиналы) на бумажном носителе (в кол-ве 4-х экземпляров) на русском языке.

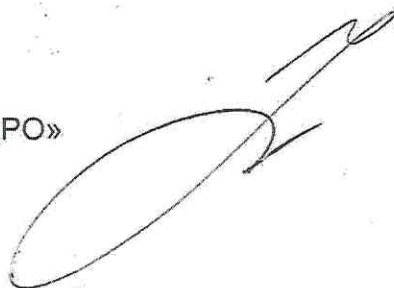
9. Срок выполнения проекта

По календарному плану к договору.

10. Заказчик

Филиал ООО «ЭН+ ГИДРО» «Усть-Илимская ГЭС».

Директор Филиала ООО «ЭН+ ГИДРО»
«Усть-Илимская ГЭС»



А.А. Карпачев

Типовая схема информационно-вычислительных сетей

