СОДЕРЖАНИЕ

СОДЕРЖАНИЕ ... 3
1 ОБЩИЕ СВЕДЕНИЯ ... 4
1.1 Полное наименование системы управления и ее условное обозначение ... 4
1.2 Основание для создания системы ... 4
1.3 География расположения системы ... 4
2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ ... 5
2.1 Назначение системы ... 5
2.2 Цель создания системы ... 5
3 ХАРАКТЕРИСТИКА ОБЪЕКТА АВТОМАТИЗАЦИИ ... 7
3.1 Краткое описание объекта автоматизации ... 7
3.2 Сведения об условиях эксплуатации системы ... 8
4.1 Требования к системе в целом ... 9
4.1.1 Требования к структуре и функционированию системы ... 9
4.1.2 Требования по сохранности информации при авариях ... 14
4.1.3 Требования к надежности ... 15
4.1.4 Требования по обеспечению информационной безопасности ... 17
4.1.5 Требования к эргономике и технической эстетике ... 17
4.1.6 Требования к безопасности ... 18
4.1.7 Требования к защите от влияния внешних воздействий ... 19
4.1.8 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы ... 19
4.1.9 Требования по стандартизации и унификации ... 21
4.2 Требования к функциям (задачам), выполняемым системой ... 22
4.2.1 Объем автоматизации ... 22
4.2.2 Функции системы ... 22
4.3 Требования к видам обеспечения ... 28
4.3.1 Требования к техническому обеспечению ... 28
4.3.2 Требования к программному обеспечению ... 36
4.3.3 Требования к метрологическому обеспечению ... 37
4.3.4 Требования к информационному обеспечению ... 39
4.3.5 Требования к математическому обеспечению ... 40
5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ АСУТП ... 42
5.1 Выбор поставщика АСУТП ... 42
5.2 Документация ... 44
5.3 Проверка и испытания АСУТП ... 45
6 НОРМАТИВНЫЕ ДОКУМЕНТЫ ... 48
7 ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ ... 50
Приложение А Требования к интерфейсу оператора ... 51
Приложение Б Перечень документов, необходимых для конфигурирования системы управления ... 56
Приложение В Требования по поставке оборудования и услуг ... 57
Приложение Г Предварительная сводная таблица входных-выходных сигналов АСУТП ... 59
Приложение Д Структурная схема комплекса технических средств (КТС) АСУТП ... 60
Приложение Е Перечень документов технорабочего проекта и эксплуатационных документов, которые должны быть переданы Поставщиком Заказчику при внедрении АСУТП ... 62
Приложение Ж Перечень отчетной документации, оформляющейся в процессе приемки и монтажа оборудования АСУТП, проведения всех видов испытаний и по их завершению ... 65
Приложение З Перечень инжиниринговых работ по АСУТП, выполняемых поставщиком ... 66
Приложение И Перечень пусконаладочных работ и испытаний по АСУТП, выполняемых поставщиком ... 69
Приложение К Пример структурной схемы электропитания АСУТП ... 72
Приложение Л Планы размещения оборудования АСУТП ... 73
Приложение М Требования по обеспечению информационной безопасности АСУТП ... 74

1 ОБЩИЕ СВЕДЕНИЯ

Настоящие технические требования (далее ТТ) на модернизацию (замену) автоматизированной системы управления технологическими процессами (далее АСУТП) объекта «Газотурбинная установка – тепловая электростанция» на РН-Туапсинский НПЗ» (далее Объект) определяют требования: на разработку, поставку и внедрение автоматизированной системы управления.

1.1 Полное наименование системы управления и ее условное обозначение

Полное наименование системы управления – «Автоматизированная система управления технологическими процессами объектом «Газотурбинная установка – тепловая электростанция» на «РН-Туапсинский НПЗ».

Условное обозначение: АСУТП ГТУ-ТЭС/Система.

1.2 Основание для создания системы

Система создается на основании нормативных документов, указанных в пункте 6 данных Технических Требований, исходных данных, предоставляемых Заказчиком, рабочей документации, разрабатываемой и предоставляемой фирмой-поставщиком вместе с оборудованием центральной части системы управления.

Основанием для проектирования являются:

- Задание на проектирование на оказание услуг на проведение технико-экономических расчётов стоимости технического перевооружения АСУТП на объекте «Газотурбинная установка – тепловая электростанция» (тит.871-10) ООО «РН-Туапсинский НПЗ»».

Разработчик ТТ на АСУТП объекта – АО «Самаранефтехимпроект», 443110, г. Самара ул. Ново-Садовая, д.11.

Технические Требования на АСУТП Объекта разрабатываются в соответствии с положением ПАО “НК “Роснефть” о Разработке технических требований на создание автоматизированной системы управления технологическими процессами № П3-04 Р-0106 версия 2.00.

1.3 География расположения системы

Место расположения системы: промышленная площадка ГТУ-ТЭС ООО «РН-Туапсинского НПЗ».

Заказчик АСУТП – ООО «РН-Туапсинский НПЗ», 352800, Краснодарский край, г. Туапсе, ул. Сочинская, д. 1

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1 Назначение системы

Модернизируемая АСУТП Объекта предназначена для автоматизированного контроля и управления агрегатами и автоматического регулирования параметров технологического и электротехнического оборудования и схем ГТУ-ТЭС на ООО «РН-Туапсинский НПЗ».

2.2 Цель создания системы

АСУТП Объекта разрабатывается как информационно-управляющая человеко-машинная система, рассчитанная на длительное функционирование в реальном масштабе времени.

АСУТП Объекта предназначена для автоматизированного управления технологическим процессом.

ГТУ-ТЭС является теплоэлектростанцией и опасным производственным объектом. Принципы построения системы и выбираемые КТС должны соответствовать требованиям к ОПО и к теплоэлектростанциям.

Основной целью создания АСУТП Объекта является:

- обеспечение выполнения установленных заданий по объемам и качеству выработки тепловой и электрической энергии;
- повышение надежности работы основного и вспомогательного оборудования, снижения риска аварий;
- обеспечение автоматизированного эффективного управления технологическими процессами качеству выработки тепловой и электрической энергии в нормальных, переходных, предаварийных и аварийных режимах работы;
- защита технологического оборудования и обслуживающего персонала при угрозе аварии;
- своевременное представление оперативному персоналу достаточной и достоверной информации о ходе технологического процесса, состояния оборудования и технологических средств управления;
- обеспечение персонала ретроспективной технологической информацией для анализа, оптимизации и планировании работы оборудования и его ремонта;
- обеспечение интеграции специализированных систем управления (ССУ) в единый комплекс АСУТП;
- улучшение условий труда эксплуатационного персонала;
- повышение экологической безопасности производства.

При создании АСУТП должны учитываться критерии эффективности АСУТП:

- экономичность работы оборудования, эффективность ведения технологического процесса, оптимизация нестандартных режимов работы и сокращение времени выполнения пусковых операций;
- затраты на ремонт оборудования, определяемые надежностью оборудования и эффективностью планирования его ремонтов;
- затраты на технические средства АСУТП, определяемые темпами ввода и освоения АСУТП.

Улучшение показателей функционирования АСУТП должно быть достигнуто благодаря применению более совершенных программных средств, обеспечивающих:

- реализацию эффективных алгоритмов управления и регулирования;
- улучшение связи (интерфейса) «человек-машина»;
- расширение информационных функций АСУТП;
- улучшение диагностики технологического оборудования и средств АСУТП;
- упрощение технического обслуживания системы контроля и управления;
- упрощение управления оборудованием.

Создание АСУТП Объекта позволит осуществлять:

- устойчивую работу системы управления технологическим оборудованием;
- уменьшение интенсивности колебаний и амплитуды случайных колебаний технологических параметров;
- повышение уровня эксплуатации за счет унификации технических и программных средств;
- повышение надежности системы управления за счет применения микропроцессорных устройств и непрерывности диагностики технических и программных средств.

3 ХАРАКТЕРИСТИКА ОБЪЕКТА АВТОМАТИЗАЦИИ

3.1 Краткое описание объекта автоматизации

Объектами автоматизации являются:

- шесть газотурбинных установок ГТУ-1…ГТУ-6 SIEMENS SGT-800 с котлами-утилизаторами, генераторами, вспомогательными системами: диверторы, система воздушного охлаждения масла АВОМ, противообледенительная система ПОС, автоматизация здания электрооборудования ЗЭО;
- два паровых котла с камерным сжиганием газового топлива;
- одна турбина противодавления с генератором и вспомогательными системами;
- насосы, деаэраторы, подогреватели, вентиляторы, дымососы и прочее вспомогательное оборудование;
- системы магистральных коллекторов и оборудование выдачи пара потребителю;
- главные распределительные устройства КРУЭ-110 кВ, распредустройства и другое электрооборудование;
- пункт подготовки газа ППГ;
- компрессорная станция приборного воздуха;
- теплоцентр с конденсатной станцией;
- отдельные комплексы общестанционного оборудования: паропроводы, газопроводы, БРПГ (блок редуцирования природного газа), стенды химанализа, газоанализ уходящих газов, редуцирующие устройства (БРОУ, РОУ, РОУ МЦК), дизельное хозяйство.

В качестве основного средства отображения информации и для оперативного управления объектом автоматизации предусмотреть станции оператора на базе персональных компьютеров, оснащенные необходимыми средствами коммуникации и специализированным программным обеспечением. Связь между операторной и аппаратной осуществлять с помощью дублированных шин управления. Для удобства визуализации технологического процесса предусмотреть обзорные экраны в операторной

3.2 Сведения об условиях эксплуатации системы

Новое оборудование Системы (шкафы, система ИБП и т.д.), предусматриваемое в рамках модернизации системы, будет размещаться в помещениях Объекта. В помещениях поддерживается температура воздуха + (18…22) °С, относительная влажность (40-60) % без конденсации влаги. Отопление обеспечивается постоянно действующей приточной вентиляцией с пятикратным воздухообменом. Для обеспечения климатических условий в летний период в помещениях управления предусмотрены резервированные сплит-системы кондиционирования. Операторские станции будут размещаться в операторной Объекта. В помещении операторной поддерживается температура воздуха (+22…+24) °С, относительная влажность (40-60) %. Отопление обеспечивается постоянно действующей приточной вентиляцией с пятикратным воздухообменом.

Технические средства системы должны быть устойчивы к воздействиям температуры и влажности окружающего воздуха:

- температура окружающего воздуха от +15 до +40 °С;
- относительная влажность от 40 до 90 % при температуре +25 °С;
- атмосферное давление от 750 до 770 мм. рт. ст.

4 ТРЕБОВАНИЯ К СИСТЕМЕ

4.1 Требования к системе в целом

АСУТП Объекта должна создаваться на базе унифицированных комплексов технических средств (КТС) контроля, управления, защиты и противоаварийной защиты.

Режим функционирования АСУТП – непрерывный с периодическими осмотрами и регламентными работами в период плановых остановов и ремонтов основного оборудования.

АСУТП должна быть реализована как распределенная, иерархическая, многофункциональная, программируемая автоматизированная система контроля, управления и противоаварийной защиты.

Разрабатываемая система должна соответствовать ГОСТ 24.104-2023 «Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования», федеральным нормам и правилам в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств» утвержденные Приказом №533 Федеральной службы по экологическому, технологическому и атомному надзору от 15 декабря 2020 года.

Документация на АСУТП должна быть выполнена в соответствии с требованиями комплекса стандартов и руководящих документов на автоматизированные системы (см. п.6).

Программные и технические средства, входящие в состав Системы, должны соответствовать требованиям Постановления Правительства РФ от 14.11.2023 № 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».

4.1.1 Требования к структуре и функционированию системы

АСУТП Объекта должна иметь следующую трехуровневую структуру:

1. Нулевой уровень – уровень оборудования КИПиА, исполнительных механизмов, многофункциональных измерительных «интеллектуальных» полевых устройств типа SENTRON, SIPROTEC (в поставку не входят).
2. Первый уровень. Уровень автоматического контроля и регулирования, защиты и блокировки на базе микропроцессорных контроллеров для обработки аналоговой и дискретной информации о ходе технологического процесса, в том числе серверное оборудование для связи между удаленными друг от друга объектами управления, а так же для сбора информации от «интеллектуальных» полевых устройств;

3. Второй уровень. Уровень операторского интерфейса, обеспечивающий максимальную доступность технологического процесса для оператора-технолога при выполнении им функций контроля и управления, состоящий из операторских станций и обзорных экранов.

Сетевая организация Системы должна обеспечивать связь с системой диспетчеризации посредством подключения к корпоративной вычислительной сети Заказчика по защищенному каналу (через шлюзы или аппаратные межсетевые экраны). Для обмена данными с заводской информационной сетью в системе необходимо предусмотреть OPC сервер (OPC DA/UA) и межсетевой экран.

Архитектура построения Системы должна исключать наличие узлов (единичных элементов и связей), отказ которых приведёт к отказу АСУТП в целом. Для обеспечения минимальной вероятности отказов должно быть предусмотрено резервирование ответственных элементов и сетей системы.

Линии связи должны быть резервированы, причем при выходе из строя одной из линий, не должна быть нарушена работа всей Системы.

Предлагаемая структурная схема КТС АСУТП приведена в **Приложении Д** данных Технических требований.

Система должна обеспечивать:

- централизованный контроль состояния процесса и сигнализацию отклонения параметров от нормы;
- управление отдельными узлами процесса по специальным алгоритмам, ручное и дистанционное управление процессом;
- передачу данных в заводскую сеть данных по протоколу OPC DA/UA.
- защиту технологического оборудования и персонала в аварийных ситуациях путем перевода технологического процесса в безопасное состояние;
- формирование журнала отчетности по аварийным сообщениям и срабатыванию блокировок (определение первопричины срабатывания блокировки);
- определение последовательности срабатывания защиты и блокировки;
- регистрация на печати и в журнале аварийных сообщений состояния процесса;
- перевод системы после срабатывания в исходное состояние

Более подробные требования к функциям изложены в разделе 4.2.2

В Системе должна быть реализована возможность изменять программную конфигурацию контроллеров и модулей системы без оказания воздействия на технологический процесс, изменения должны осуществляться в режиме on-line.

Система должна быть построены на базе унифицированных комплексов технических средств (КТС), имеющих:

- свидетельство об утверждении типа средств измерений выданные Федеральным агентством по техническому регулированию и метрологии (РОССТАНДАРТ);
- Сертификаты соответствия требованиям Технического регламента Таможенного союза (ТР ТС 004/2011, ТР ТС 012/2011, ТР ТС 010/2011, ТР ТС 020/2011) или аналогичные сертификаты соответствия требованиям Технических регламентов Евразийского экономического союза (ТР ЕАЭС).

Система должна иметь аппаратную и программную диагностику исправности сетей, станций, блоков, модулей. В Системе для резервированных модулей и блоков должна быть предусмотрена возможность замены неисправных модулей и блоков в оперативном режиме работы (ON-LINE) без нарушения функционирования Системы.

Система должна иметь возможность передачи любой технологической информации в систему диспетчеризации предприятия.

Согласно «Правил работы с персоналом в организациях электроэнергетики РФ», пункта 12, 13 параграфа II должен быть создан тренажёрный комплекс для обучения оперативного персонала управлению ГТУ-ТЭС Туапсинского НПЗ в нормальных и нештатных режимах, как при полном объеме работающих функций АСУТП, так и при их частичном отключении (режим дистанционного управления при отдельных или массовых отказах функций автоматизации). Основной целью создания тренажера является разработка, наладка и ввод в эксплуатацию полномасштабного тренажера оперативного персонала ГТУ-ТЭС, в полном объеме моделирующего как АСУТП на базе современного ПТК, так и с высокой точностью технологические процессы ГТУ-ТЭС.

В диспетчерском пункте здания инженерно-бытового корпуса ГТУ-ТЭС должны размещаться:

- девять автоматизированных рабочих места оператора-технолога (АРМ ОТ);
- одна инженерная станция (ИС);
- одна ИС резервного копирования;
- принтеры;
- специализированная мебель для размещения АРМ и принтеров;

В помещении ИБК инженерно-бытового корпуса ГТУ-ТЭС размещаются:

- шкафы: системные, кроссовые, терминальные;

- шкафы сетевые/коммуникационные в комплекте с оборудованием для организации связи оборудования первого уровня и нулевого уровня Системы, для связи с внешними сетями;
- АРМ администратора;
- ОРС сервер и межсетевой экран;
- сервер точного времени;
- система бесперебойного электропитания АСУТП (включая шкафы ввода/байпаса);
- шкафы распределения питания, в том числе и те, которые поставляются комплектно с технологическим оборудованием.

Предварительные планы расположения оборудования АСУТП показаны в **Приложении Л.**

Существующая структура Системы предполагает наличие шкафов удаленного ввода-вывода, располагаемых на технологических объектах. К шкафам подключаются существующие полевые приборы, исполнительные механизмы, многофункциональные измерительные «интеллектуальные» полевые устройств типа SENTRON, SIPROTEC.

Предположительное назначение шкафов:

- шкафы для ГТУ-1…ГТУ-6;
- шкафы для дивертеров 1…6. На дверях шкафов должны быть сенсорные ЖК-панели для управления;
- шкафы котлов-утилизаторов КУ-1…6;
- шкафы система воздушного охлаждения масла АВОМ-1…6. На дверях шкафов должны быть сенсорные ЖК-панели для управления;
- шкафы противообледенительной системы ПОС-1…6. На дверях шкафов должны быть сенсорные ЖК-панели для управления;
- шкафы автоматизация здания электрооборудования ЗЭО-1…6. На дверях шкафов должны быть сенсорные ЖК-панели для управления;
- шкаф для паровых котлов ПК-1 и ПК-2
- шкаф общекотельной части;
- шкаф для паровой турбины
- шкаф общестанционной части и шкаф РОУ МЦК;
- шкаф теплоцентра;
- шкаф пункта подготовки газа ППГ. На дверях шкафа должна быть сенсорная ЖК-панель для управления;

– шкаф компрессорной станции приборного воздуха КСПВ. На дверях шкафа должна быть сенсорная ЖК-панель для управления.

Шкафы в приоритете сохранить, монтаж вновь проектируемых компонентов осуществить в текущих шкафах. Максимально сохранить существующие схемы питания компонентов. По возможности сохранить всю сетевую структуру с магистральными связями между объектами. Если данные условия невыполнимы Поставщиком, то Поставщик дает свои предложения по размещению новых шкафов.

Также необходимо предусмотреть локальные АРМ ОТ:

– шесть АРМ турбин, располагаемых в помещениях САУТ ГТУ 1-6;
– одно АРМ, располагаемое в пункте подготовки газа ППГ;
– одно АРМ, располагаемое в теплоцентре.

Разрабатываемая АСУТП должна считаться соответствующей ее назначению при удовлетворении следующих показателей:

– обеспечивается (автоматически) во всех режимах работы технологического оборудования надежная защита эксплуатационного персонала, действующего оборудования и окружающей среды от возможных аварий;
– обеспечивается индивидуальное дистанционное управление любым исполнительным механизмом, включенным в состав АСУТП;
– обеспечивается автоматический контроль и регулирование технологических параметров при работе технологического оборудования в регулировочном диапазоне параметров процесса;
– обеспечивается автоматическое, удобное по форме, достаточное по объему и быстродействию отображение и регистрация информации о технологических параметрах оборудования;
– обеспечиваются заданные метрологические характеристики измерительных каналов;
– обеспечивается (автоматически) диагностика неисправностей технических и программных средств АСУТП, предотвращающая выдачу ложных команд управления технологическим оборудованием и позволяющая своевременно устранять неисправности;
– обеспечивается дальнейшее развитие системы с увеличением количества управляемых объектов.

4.1.2 Требования по сохранности информации при авариях

Система должна обеспечивать сохранность информации при отказах, авариях и других нештатных ситуациях. Системой предусмотрено архивирование и хранение проектных и текущих данных в соответствии с проектной документацией.

Возможные основные ситуации, приводящие к потере информации и меры, обеспечивающие ее сохранность и безаварийную работу системы:

- полное длительное обесточивание всей системы – в этом случае источники бесперебойного питания должны обеспечить питание рабочих станций на время, достаточное для штатного завершения работы системы с целью сохранения информации. Кроме того, должно быть предусмотрено периодическое копирование данных на внешние накопители, для контроллеров - использование энергонезависимых ПЗУ;
- полное кратковременное обесточивание всей системы - работоспособность системы в данном случае должна поддерживаться за счет использования источников бесперебойного питания. ПОСТАВЩИКОМ должно быть обеспечено сохранение всех возлагаемых на ПТК функций при наличии хотя бы одного из источников питания (основного или резервного). При потере электропитания от одного источника и его последующим восстановлении (АВР питания) не должны выдаваться ложные команды или ложная информация;
- обесточивание (отказ) отдельных контроллеров. В данном случае сохранность информации должна обеспечиваться за счет хранения текущей базы данных контроллеров в загрузочных файлах инженерной станции (сервера) и энергонезависимой памяти. Модули ввода/вывода при обесточивании (отказе) контроллера должны сохранять значения выходных сигналов для безударного ведения технологического процесса, в том числе перевод в безопасное состояние;
- отказ рабочей станции не должен приводить к потере информации, необходимой для непосредственного управления процессом в автономном режиме. В данной ситуации отсутствует лишь отображение на этой конкретной станции;
- отказ модуля ввода/вывода. В данной ситуации теряется связь с датчиком или исполнительным механизмом до момента восстановления работоспособности модуля. Отказ модуля ввода/вывода не должен приводить к использованию недостоверной информации для функций контроля, учета и управления. При отказе контура управления выход контура должен быть «заморожен» на уровне последних достоверных показаний.

В составе поставляемого ПТК должны использоваться надежные устройства внешней памяти (жесткие диски емкостью не менее 2Тб) для сохранения и восстановления ретроспективной информации.

Обеспечение надежности хранения информации может обеспечиваться также специальной технологией хранения информации в энергонезависимых устройствах памяти.

Время хранения оперативных констант – не менее 72 часов.

Информация об аварийных ситуациях должна автоматически индицироваться на дисплее АРМ ОТ, а также записываться и храниться в протоколах сообщений системы на устройствах внешней памяти.

При отказах средств связи МПК с АРМ ОТ, МПК должны функционировать в автономном режиме, а на АРМ ОТ должно появиться сообщение об отказе.

После восстановления работоспособности средств связи, обмен информацией между МПК и АРМ ОТ должен восстанавливаться автоматически с выдачей соответствующего сообщения на АРМ ОТ.

4.1.3 Требования к надежности

Показатели надежности системы должны отвечать требованиям ГОСТ 24.701-86 «Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения».

Для обеспечения безотказной работы системы управления предусмотреть резервирование («Нагруженный резерв» ГОСТ Р 27.102-2021) контроллеров Системы с кратностью резерва не менее чем один к одному (1/1).

Архитектура контроллеров Системы должна быть не хуже 1oo2D (один из двух с диагностикой).

Должно быть предусмотрено 100% резервирование внутрисистемных магистралей, сетевых устройств и линий передачи данных, 100% резервирование архивов и баз данных.

Переход на резерв должен производиться автоматически, безударно и без остановки технологического процесса. Замена неисправного модуля должна производиться без остановки технологического процесса.

Должна быть предусмотрена гальваническая развязка каналов (для каналов дискретного ввода-вывода установка промежуточных реле), модулей, шин связи.

При отказе в работе измерительного преобразователя, участвующего в контуре регулирования и характеризующегося недостоверным сигналом, поступающим в систему, должно быть предусмотрено удержание выходного сигнала на исполнительный механизм на предыдущем уровне.

Регулирующие и отсечные клапаны при исчезновении (отключении) управляющего сигнала будут занимать безопасное для технологического процесса положение в соответствии с требованиями Технологического регламента.

В Системе должна быть предусмотрена возможность хранения базы данных и файлов конфигурации системы на внешнем носителе информации и оперативной загрузки их в Систему.

Сеть управления Системой должна быть резервирована.

При применении серверной структуры АСУТП все серверные станции должны быть резервированы. Серверы базы данных АСУТП должны быть выделенными, совмещение с АРМ ОТ и ИС не допускается. Размещение серверов базы данных АСУТП согласовывается с Заказчиком.

Надежность технических средств и программного обеспечения, предназначенных для реализации каждой из функций системы, должна обеспечивать в совокупности выполнение требований по надежности функций:

- среднее время безотказной работы не менее 40 000 час;
- среднее время восстановления не более 0,2 часа.

Система должна обеспечивать диагностику своих технических средств в режиме нормальной работы.

Должны быть реализованы следующие способы повышения надежности:

- резервирование информационных линий связи;
- высокая надежность комплектующих элементов, субблоков, модулей, устройств передачи информации;
- наличие аппаратной, информационной, функциональной и алгоритмической избыточности, обеспечивающей своевременное определение и устранение причин единичных отказов;
- разработка надежно работающих программных средств;
- развитая система диагностики технических и программных средств;
- защита от выдачи ложных команд и ложной информации;
- рациональное распределение функций управления между техническими средствами и персоналом;
- использование рациональных интерфейсов «человек-система», позволяющих быстро и однозначно идентифицировать ситуацию;
- хранение наиболее важной информации и программ в энергонезависимых запоминающих устройствах и реализация постоянного контроля за целостностью хранимой информации;
- организация защиты базы данных и программного обеспечения от несанкционированного вмешательства;
- гальваническая развязка каналов, модулей, шин связи;
- организация рациональной эксплуатации ПТК АСУТП и обеспечение запасными частями;

– повышение уровня квалификации персонала.

Надежность выполнения функций на стадиях проектирования оценивается расчетным методом по характеристикам элементов, участвующих в реализации функций. На стадии внедрения надежность оценивается по фактическим статистическим данным по сбоям и отказам функций системы.

На все поставляемые технические средства в документации и в паспорте должен быть указан назначенный срок службы, или назначенный ресурс. Срок службы Системы в целом должен быть не менее 10 лет с учетом проведения восстановительных работ и работ по модернизации. Входящие в состав поставляемой АСУТП оборудование и ПО на момент поставки должно быть последней модификации, с последними обновлениями hard-ware, soft-ware, обеспечиваться технической поддержкой производителя на весь заявленный срок службы.

4.1.4 Требования по обеспечению информационной безопасности

Для обеспечения штатного режима функционирования АСУТП должен быть предусмотрен комплекс организационных и технических мер, составляющих систему защиты информации АСУТП и обеспечивающих информационную безопасность в соответствии с требованиями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», 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 и ЛНД Компании в области информационной безопасности АСУТП.

Полные требования по обеспечению ИБ АСУТП, а также ссылки на нормативную документацию по ИБ приводятся в **Приложении М**.

4.1.5 Требования к эргономике и технической эстетике

Условия работы персонала должны соответствовать ГОСТ 12.3.002-2014. Взаимодействие персонала с АСУТП осуществляется через специализированные АРМ.

Интерфейс разрабатываемой системы АСУТП должен быть интуитивно-понятным, позволяющим пользователю в кратчайшие сроки освоить работу с АСУТП. Должен быть реализован графический многооконный режим с настраиваемыми элементами интерфейса и цветового оформления.

Отображение информации на экране цветного графического дисплея должно обеспечивать получение оператором полной характеристики текущего состояния технологического процесса и оборудования и возможность управления ими в виде, наиболее удобном для восприятия в каждой конкретной ситуации. Фрагменты изображения

не должны быть перенасыщены информацией и разнообразием цветовой гаммы. Фон графических экранов должен быть не ярким и выбран из «спокойной» цветовой гаммы.

Все рабочие места должны быть оборудованы инженерной мебелью специального исполнения, которая обеспечивает удобство работы.

Общие эргономические требования к залу операторов и расположению рабочих мест должны соответствовать ГОСТ 21958-76.

Общие эргономические требования, регламентирующие организацию рабочего места в рамках поставляемой мебели – согласно ГОСТ 22269-76.

4.1.6 Требования к безопасности

Требования к безопасности ПТК АСУТП должны соответствовать требованиям раздела 2 ГОСТ 24.104-2023, а также требованиям безопасности, определенным ФНиП «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств».

В соответствии ФНиП «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств», контроллеры и компоненты ПАЗ должны соответствовать требованиям функциональной безопасности по ГОСТ Р МЭК 61508.

Технические средства ПТК АСУТП, по требованиям защиты человека от поражений электрическим током относятся к классу 1, должны выполняться в соответствии с ПУЭ, ГОСТ-12.2.007.0-75, ГОСТ Р 50571.4.41-2022 и ГОСТ 25861-83.

Конструкция и размещение стоек (шкафов) МПК должны удовлетворять требованиям электробезопасности в соответствии ГОСТ-12.1.030-81 «Система стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление».

Стойки (шкафы) должны быть оснащены механическими блокираторами дверей (крышек), исключающими их самопроизвольное или несанкционированное открытие. ЗАКАЗЧИК должен принять организационные меры к сохранности элементов ПТК.

Конструктивные элементы стоек (блоков) должны исключать возможность прикосновения к токоведущим частям, а также замыкания на корпус и накоротко, и иметь предупредительные надписи и гравировки на русском языке.

Степень защиты шкафов - не менее IP20. Шкафы должны закрываться на ключ и ручки шкафов должны быть без выступающих частей (утопленная ручка, выдвигаемая после поворота ключа).

Мониторы АРМ ОТ должны соответствовать требованиям Российских санитарных норм «СанПиН 2.2.2/2.4.1340-03: Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

Для защиты обслуживающего персонала и ПТК АСУТП от возникновения разности потенциалов на контуре заземления в местах установки разнесенного оборудования,

вызванного короткими замыканиями в электрической части, атмосферными разрядами, протеканием уравнительных токов по контуру заземления и т.п. должны предусматриваться заземление компонентов КТС АСУТП в соответствии с ПУЭ.

4.1.7 Требования к защите от влияния внешних воздействий

Ввиду установки оборудования АСУТП в отапливаемых помещениях с обеспечением необходимого микроклимата, особых требований к защите от воздействия окружающей среды не предъявляется.

АСУТП должна быть устойчива к воздействию внешних магнитных полей, постоянных или переменных с частотой сети с напряженностью до 400 А/м.

АСУТП должна сохранять работоспособность при воздействии индустриальных радиопомех по нормам 8-95 «Радиопомехи индустриальные».

Для обеспечения защиты от внешних воздействий, технические средства АСУТП (контроллеры, модули ввода/вывода, ИБП, преобразователи интерфейсов) должны быть установлены в закрытых металлических шкафах/и/или боксах, оборудованных запорными устройствами.

4.1.8 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

АСУТП должна эксплуатироваться в режиме круглосуточной непрерывной работы. Профилактическое и ремонтное обслуживание отдельных частей АСУТП должно проводиться во время остановки на профилактическое и ремонтное обслуживание контролируемого технологического оборудования.

Должны быть предусмотрены следующие виды технического обслуживания и ремонта:

a) Оперативный контроль исправности АСУТП, который автоматически в режиме on-line должен обеспечивать:
   - выявление факта неисправности, в том числе отсутствия электропитания;
   - прием в АСУТП диагностических сообщений от полевых приборов с представлением на операторскую станцию обобщенного сигнала о неисправности и ее характере;
   - определение места неисправности до сменного модуля;
   - контроль состояния сети управления АСУТП, а также контроль целостности цепей датчиков и исполнительных устройств;
   - функциональный контроль статуса входных сигналов по границам допустимого изменения параметров.

b) Регламентный контроль исправности АСУТП, должен производиться при выводе аппаратуры из действия и в общем случае обеспечивать контроль датчиков и тестовую проверку аппаратуры всех типов, включительно до сменного модуля, проверку каналов

управления и контуров регулирования. Для обеспечения регламентного контроля в значительной мере должны использоваться средства, предусмотренные для оперативного контроля. Обобщенная информация о неисправности должна представляться на операторскую станцию.

c) Плановое техническое обслуживание.

Периодичность технического обслуживания и объем контролируемых параметров АСУТП, необходимых для технического обслуживания и ремонта, должны быть определены на этапе создания АСУТП и представлены в эксплуатационной документации.

Удобство технического обслуживания и ремонта АСУТП должно обеспечиваться:

- свободным и удобным доступом к модулям и другим восстанавливаемым элементам и монтажу;
- укомплектованностью ЗИП;
- возможностью применения стандартных приспособлений для демонтажа и монтажа;
- использованием конструктивных принципов, исключающих неправильное выполнение операций технического обслуживания, а также маркировкой и окраской в различный цвет однотипных деталей, предназначенных для выполнения разных функций и т.п.;
- возможностью контроля и регулировки параметров аппаратуры при помощи встроенных или переносных средств контроля;
- взаимозаменяемостью однотипных блоков и модулей без дополнительной регулировки и настройки;
- возможностью оперативного внесения изменений в процессе сдачи и эксплуатации по причинам возникновения изменений в управляемых системах, комплексах и технических средствах.

В эксплуатационной документации должны быть указаны виды технического обслуживания и ремонта и обеспечение их ЗИП, периодичность, продолжительность, трудоемкость и квалификация персонала, а также, при необходимости, перечень переносной контрольно-проверочной аппаратуры и инструкции по ее применению.

Полный перечень ЗИП должен быть определен на основании требований раздела 5.1, приложения В и приведен в рабочей документации в «Ведомости ЗИП».

В комплект поставки АСУТП должны входить: комплект внешних диагностических устройств, комплект специального инструмента и монтажных приспособлений для выполнения всех операций по монтажу, наладке эксплуатации и ремонту оборудования.

Условия хранения ЗИП и аппаратуры АСУТП (до ее монтажа) должны соответствовать ГОСТ Р 52931-2008.

Условия хранения носителей с копиями ПО должны соответствовать паспортным данным носителей.

Транспортирование и хранение технических средств АСУТП должны соответствовать требованиям ГОСТ Р 52931-2008.

4.1.9 Требования по стандартизации и унификации

Аппаратура АСУТП должна быть спроектирована с максимальной унификацией решений. Унификация всех решений должна обеспечиваться единообразным подходом к решению однотипных задач, созданием унифицированных объектно-ориентированных компонентов технического, программного, информационного, лингвистического обеспечения.

Конструктивы шкафов, функциональных модулей должны быть унифицированы во всех устройствах комплекса технических средств АСУТП. Должна использоваться минимальная номенклатура различного оборудования.

Должно использоваться минимальное количество номиналов питающих напряжений.

В инструментальной системе должны использоваться универсальные операционные системы и технологические языки программирования высокого уровня.

Формы представления информации должны быть максимально приближенными к проектным изображениям технологических схем и их элементов.

Технологические алгоритмы должны разрабатываться в формализованном виде на специализированном языке, доступном специалистам-технологам.

4.2 Требования к функциям (задачам), выполняемым системой

4.2.1 Объем автоматизации

Объем автоматизации определяется в соответствии с количеством входных/выходных технологических параметров, количеством параметров сигнализации, регулирования, управления и количеством блокировок. Сводный перечень входных-выходных сигналов представлен в **Приложении Г**.

4.2.2 Функции системы

АСУТП технологического объекта должна обеспечивать выполнение следующих функций:

- автоматизированный сбор и первичная обработка технологической информации, определение значений параметров по измеренным сигналам;
- формирование команд управления;
- накопление, регистрация и хранение поступающей информации;
- предупредительная и аварийная сигнализация при выходе технологических параметров за установленные границы и при обнаружении неисправностей в работе оборудования АСУТП;
- визуализация хода и результатов процесса;
- автоматическое составление отчетов и рабочих (режимных) листов за определенные периоды времени.

Оперативный контроль значений технологических параметров с заданной частотой сканирования

- сбор и первичная обработка сигналов с объекта управления;
- контроль достоверности входной информации по следующим условиям:
    - короткое замыкание;
    - обрыв цепи датчика;
    - превышение скорости изменения (при необходимости);
- сглаживание и фильтрация сигнала с помехами (при необходимости);
- отказ микропроцессорных контроллеров;
- обрыв одного из проводов резервируемой сети;
- потеря связи между контроллерами;
- отказ рабочих станций, как оборудования, так и программного обеспечения;
- отказ источников питания;
- формирование значений параметров в относительных и инженерных единицах;
- пересчет шкалы (при необходимости);

- корректировка объемных расходов по температуре и давлению;
- взаимный пересчет объемных и массовых расходов (при необходимости);
- расчет среднеинтегральных значений параметров на заданном интервале времени.

АСУТП должна обеспечивать диагностику и самодиагностику технических средств в режиме нормальной эксплуатации:

- возможность выполнения тестирования всех элементов системы в любой момент времени по команде инженера АСУТП;
- возможность проверки работоспособности датчиков и преобразователей (в том числе с использованием интерфейса HART).

Диагностика должна выявлять возникновение отказа с точностью до типового элемента замены. Информация обо всех выявленных неисправностях должна выдаваться на АРМ оператора и сопровождаться сигнализацией и цветовым выделением неисправного элемента на мнемосхеме. Неисправное оборудование должно четко идентифицироваться на мнемосхеме с точностью до канала модуля.

При обнаружении недостоверного входного сигнала система должна выдать сообщение оператору о неисправности, сигнал должен удерживаться системой на уровне, соответствующем последнему достоверному значению входного сигнала. Если параметр задействован в контуре автоматического регулирования, регулятор должен перейти с автоматического режима регулирования в ручной, управляющий сигнал указанного контура должен удерживаться системой на уровне, соответствующем последнему достоверному значению входного сигнала.

Общее время, затраченное системой управления на считывание информации на входе, обработку алгоритма управления и передачу полученного результата на выход системы управления для всех аналоговых сигналов не должно превышать 1 секунды.

АСУТП не должна самопроизвольно включать или выключать (открывать или закрывать) исполнительные устройства при любых неисправностях системы.

Автоматическое регулирование технологического процесса

- регулирование по ПИД-закону в режиме непрерывного управления;
- каскадное и многосвязное регулирование;
- безударный переход при изменении режимов регулирования;
- выполнение технологических ограничений на диапазон изменения положения клапана в процессе регулирования.

Контуры управления должны работать детерминировано с заданным временем цикла управления по замкнутому контуру.

Автоматическое управление технологическим процессом

- оперативное изменение статуса контура регулирования по команде оператора (Ручной, Автоматический, Каскадный) при условии безударного перехода;
- оперативное изменение задания в любом контуре регулирования по команде оператора;
- управление технологическим процессом непосредственно с фрагмента мнемосхемы с помощью клавиатуры и манипулятора «мышь»;
- запуск с пульта операторской станции управляющих программ и логических последовательностей;
- управление электроприводом по технологическим параметрам согласно алгоритмам;
- система должна при необходимости иметь возможность выполнять управления, когда задание регулятора формируется в результате выполнения вычислительной процедуры непосредственно в микропроцессоре управляющего контроллера с частотой сканирования процесса.
- контроль значений порогов блокировок.

Дистанционное управление с пульта операторской станции

- управление положением исполнительных механизмов (регулирующих клапанов, клапанов- отсекателей, задвижек и др.);
- останов и пуск насосов, вентиляторов, электрооборудования.
- звуковая и световая сигнализация о состоянии технологического процесса и АСУТП
- формирование групп параметров предупредительной и предаварийной сигнализации в соответствии с требованиями технологии;
- оповещение персонала о нарушении норм технологического регламента с регистрацией в журнале событий и, при необходимости, на печатающем устройстве;
- оповещение персонала об изменении состояния технологического оборудования, отображение на экранах рабочих станций положения деблокировочных ключей с регистрацией изменения их состояния в журнале событий и, при необходимости, на печатающем устройстве;
- назначение соответствующей тональности или уровня звукового сигнала и светового воздействия на оперативный персонал в зависимости от приоритетности причин сигнализации;
- изменение цвета и перевод в «мигающий» режим фрагментов мнемосхем при срабатывании предупредительной и предаварийной сигнализации;
- появление предупреждающих или директивных надписей на мнемосхемах технологического процесса.

сигнализация должна производиться:

- миганием графического отображения технологического оборудования соответствующим цветом;
- включением звукового сигнала;
- записью причины и времени срабатывания сигнализации в журнал сигнализации, а также времени квитирования сигналов сигнализации;
- появлением на экране сообщения с причиной сигнализации;
- возможность реализации функции запроса подтверждения действий оператора

Отображение технологической и системной информации на экранах операторских станций

- отображение совокупности данных, относящихся к отдельному параметру или контуру регулирования;
- отображение данных, относящихся к группе параметров;
- представление обзорного дисплея для определения состояния сформированных групп параметров;
- анимация графических объектов (элементов) на мнемосхеме с заданной степенью детальности;
- представление одиночных и групповых трендов параметров с заданной продолжительностью предыстории;
- отказ оборудования АСУТП;
- отключение внешнего электропитания и переход на резервное электропитание.
- формирование системных сообщений о состоянии управляющего комплекса, выполняемых функциях, результатах прохождения диагностических тестов.

Текстовое оповещение о событиях (технологическая сигнализация, системное сообщение и т.п.) должно отображаться в специальной строке графического интерфейса Системы.

Действие звуковой сигнализации и мигание изображения параметра (оборудования) должно продолжаться до момента квитирования (подтверждения) сообщения оператором. Цветовая индикация отклонений на мнемосхеме и отображение отклонений на экране текущей аварийной сигнализации должны сохраняться до тех пор, пока значение параметра не войдет в норму.

Накопление технологической информации

- формирование трендовых групп параметров;
- архивация значений параметров с дискретностью не более 1 секунд; срок хранения исторических данных не менее 12 месяцев;
- формирование журнала событий для регистрации действий операторов, срабатываний блокировок, включения-выключения технологического оборудования;

- формирование текущих, сменных, суточных, месячных, хозрасчетных рапортов по заданной форме;
- формирование отчетов о нарушении режима;
- хранение базы данных контроллеров;
- формирование текстовых сообщений технологической сигнализации в понятной терминологии;
- архивация сообщений сигнализации в единый журнал с возможностью удобного поиска и обработки массива информации, в том числе с использованием фильтров;
- возможность периодической записи архивной информации по всем видам данных на жесткий носитель в архив длительного хранения по команде инженера АСУТП. Объем сохраняемой информации определяется инженером АСУТП.
- для всех позиций прямо или косвенно (давление, температура, плотность и др.) участвующих в расчете материального баланса, должны быть созданы отдельные теги для накопителей: динамический накопитель, сменный (для каждой смены), суточный, месячный. Значения тега сменного, суточного и месячного накопителя должны сохранять свои значения до следующего соответствующего периода. Данные теги должны быть внесены в накопление истории (трендов).

Суточный режимный лист автоматически выводится на печать один раз в сутки в указанное время, содержит информацию по режимным переменным.

Отчет о нарушении режима конфигурируется средствами системы, вызывается на печать по требованию персонала, хранится в системе не менее трех суток.

Отчет по хозрасчетным параметрам выводится на печать один раз в сутки средствами системы по списку.

Формы вышеназванных документов предоставляет пользователь системы управления в соответствии с принятыми у Заказчика.

Автоматическая защита технологического оборудования при нарушении норм технологического регламента

- частичный или полный останов технологического процесса и блокировка технологического оборудования в аварийных ситуациях;
- определение причины срабатывания защиты и блокировки;
- определение последовательности срабатывания защиты и блокировки;
- регистрация в журнале событий и/или на печати состояния блокировочных ключей;
- перевод системы защиты и блокировки после срабатывания в исходное состояние с пульта операторской станции.

Возврат в исходное положение всех исполнительных механизмов, используемых в схемах блокировки, должен производиться по технологическому алгоритму или по команде оператора.

Обмен технологической и системной информацией через общезаводскую информационную сеть

- передача технологической информации в систему диспетчеризации предприятия с помощью станции диспетчеризации (через аппаратный межсетевой экран);

4.3 Требования к видам обеспечения

4.3.1 Требования к техническому обеспечению

Комплекс технических средств (КТС) должен быть достаточным для реализации заложенной структуры и функций разрабатываемой системы. Система управления должна обеспечить непрерывное ведение технологического процесса, сохранять свои основные функции при выходе из строя отдельных элементов системы и позволять проводить текущий ремонт или замену элементов без остановки технологического оборудования.

Система должна обеспечить диагностику и самодиагностику своих технических средств в режиме нормальной эксплуатации:

- возможность тестирования всех элементов в любой момент времени;
- возможность проверки работоспособности датчиков и преобразователей.

Диагностика должна выявлять возникновение отказа с точностью до типового элемента замены.

Технические средства системы включают:

- первичные (и вторичные) измерительные преобразователи (датчики);
- средства передачи информации (кабельные линии связи) от датчиков к МПК, технические средства микропроцессорных контроллеров (МПК);
- средства передачи информации (цифровую линию связи) от МПК к АРМ ОТ с производительностью не менее 100 Мб/с;
- технические средства АРМ ОТ;
- технические средства ИС;
- средства электропитания КТС МПК, АРМ ОТ, ИС, первичных (и вторичных) измерительных преобразователей.

Программно-аппаратный уровень цифрового обмена HART может быть реализован как в модулях ввода/вывода, так и с использованием внешних устройств (мультиплексоров и пр.)

В качестве основы для комплектации АРМ ОТ должны использоваться современные рабочие станции, состав которых обеспечит выполнение предъявляемых к АСУТП требований с заданным быстродействием и надежностью. В качестве основы для обеспечения надежного электропитания КТС МПК и АРМ ОТ должны использоваться источники бесперебойного питания (ИБП).

Программно-технические средства первого уровня обеспечивают связь с объектами, обработку и подготовку информации для реализации задач контроля и управления.

Технические средства первого уровня включают в себя:

- микропроцессорные контроллеры нижнего уровня (МПК) со своими устройствами

связи с объектами (УСО), осуществляющие реализацию алгоритмов контроля и управления, а также средства связи с АРМ ОТ.

МПК работают под контролем АРМ ОТ, а также автономно и выполняют следующие функции:

- прием и обработку входных аналоговых и дискретных сигналов, получаемых от преобразователей, от «сухих» контактов и т.п.;
- контроль достоверности поступающей информации;
- гальваническое разделение входных сигналов между собой и по отношению к вычислительной части МПК;
- логическую и арифметическую обработку входной информации;
- формирование и гальваническое разделение выходных управляющих команд;
- обмен информацией с верхним уровнем контроля и управления (АРМ ОТ);
- автоматическую самодиагностику исправности технических средств и программного обеспечения с выдачей уведомлений о неисправностях.

Обмен информацией между УСО и МПК должен осуществляться автоматически по резервированной цифровой магистрали последовательного типа, образующей локальную информационно-управляющую сеть агрегатного уровня АСУТП.

Информационный обмен между МПК и АРМ ОТ должен осуществляться автоматически по резервированной высокоскоростной цифровой магистрали напрямую без промежуточных серверов.

Контроллеры Системы с функциями автоматического управления (регулирования) технологическим процессом должны иметь:

- 100% резервированные процессорные модули;
- 100% резервированные блоки питания корзин расширения (узлов, шасси);
- 100% резервированные модули связи внутренних шин управления;
- 100% резервированные аналоговые входные модули (для сигналов блокировочных позиций);
- 100% резервированные дискретные входные модули (для сигналов блокировочных позиций);
- 100% резервированные дискретные выходные модули (для сигналов блокировочных позиций).
- 100% резервированные блоки питания корзин расширения (узлов, шасси);
- 100% резервированные модули связи внутренних шин управления;

Загрузка каждого центрального процессора не должна превышать 60%.

Выполнение программы в контроллерах не должно останавливаться при любых возможных ошибках в прикладном ПО, выполненном стандартными средствами разработки данной системы. При обнаружении ошибки в одном из программных модулей, контуре, или

схеме управления, другие модули или схемы управления должны гарантированно оставаться в работе. При этом должны выдаваться информационные сообщения об обнаруженных отказах, неисправностях.

Подключение входных/выходных дискретных сигналов, не требующих искрозащиты, должно производиться через промежуточные реле. Реле должны поставляться комплектно со специализированными релейными платами, общепромышленного применения, имеющими специализированные разъемы для подключения кабелей для соединения с модулями ввода/вывода, дублированное независимое питание 24В, необходимые предохранители.

Применение модулей ввода-вывода со встроенной искрозащитой не допустимо.

Для контуров регулирования и блокировок применить одноканальные барьеры. Барьеры должны поставляться комплектно со специализированными терминальными платами, имеющими специализированные разъемы для подключения кабелей для соединения с модулями ввода/вывода в том числе и к резервированным, дублированное независимое питание 24В, необходимые предохранители.

Применение терминальных панелей барьеров/реле для более чем одного модуля ввода-вывода недопустимо.

Структура построения Системы должна соответствовать принципу: отдельная клеммная группа кроссового шкафа – отдельная терминальная панель барьеров/реле – отдельный или резервированный модуль ввода вывода.

Источники питания 24В в релейных и барьерных шкафах должны быть дублированными.

В составе контроллеров предусматриваются отдельные коммуникационные модули для связи с другими системами (порты связи RS-485, протокол Modbus TCP, протокол Profibus, протокол МЭК 61850 для связи с локальными шинами и оборудованием).

Для размещения нового оборудования АСУТП должны использоваться существующие шкафы с полной заменой внутреннего устройства.

Для размещения активного оборудования (контроллеры, модули ввода/вывода, барьеры, станции, сетевое оборудование, активное силовое оборудование и т.д.) предусмотреть возможность оборудования существующих шкафов системой принудительной вентиляцией, автоматически включающейся при повышении температуры в шкафу от допустимых эксплуатационных значений.

Каждый шкаф, оборудованный принудительной вентиляцией должен содержать внутренний датчик температуры, данный датчик должен формировать сообщения сигнализации в АСУТП при отклонении температуры.

В случае невозможности использования существующих корпусов шкафов необходимо предусмотреть новые закрытые запираемые шкафы. Требования к поставке новых шкафов представлены ниже.

Для шкафов шириной 800 мм и более должны использоваться двухстворчатые двери. Все дверцы должны быть легкосъемными, содержать уплотнения и быть достаточно жесткими во избежание деформации и коробления. Минимальный угол открывания дверей должна быть 130°.

Шкафы должны быть высотой не менее 2000 мм без учета цоколя, глубиной не более 800 мм (за исключением серверных) и шириной не менее 800 мм.

Шкафы автоматизации должны удовлетворять следующим требованиям:

- разделение по назначению:
  - отдельные системные (контроллерные) шкафы;
  - отдельные кроссовые шкафы;
  - отдельные шкафы реле/барьеров искрозащиты /преобразователей (терминальные);
- шкафы серверные;
- шкафы распределения питания;
- шкафы коммуникационные (сетевые) в комплекте с сетевыми коммутаторами и оборудованием для подключения резервированных линий связи;
- шкафы удаленных вводов-выводов, размещаемые на технологических объектах;
- выделенный шкаф распределения питания оборудования КИПиА (в комплекте с 2 парами резервированных источников питания постоянного тока по 40А каждый, устройствами АВР переменного тока, быстродействием не более 20мс, клеммниками проходными с ножевыми расцепителями, клеммниками с предохранителями, кабельными лотками, автоматическими выключателями и т.п.);
- шкаф ввода питания и байпаса ИБП;
- наличие цоколя не менее 100 мм;
- запираться на ключ;
- для питания реле и барьеров искробезопасности должны быть предусмотрены отдельные резервируемые источники питания 24В с необходимым коммутационным оборудованием (как по входу, так и по выходу), входящим в комплект поставки;
- наличие вентиляторов;
- наличие термостата;
- иметь шины защитного и сигнального заземления;
- с нижним подводом кабелей из фальшпола;
- поставляться в сборе.

Для монтажа оборудования в шкафах должны использоваться монтажные плиты (панели) или специальные профили. Для монтажа оборудования размером 19" должны использоваться специальные монтажные профили и переходники. Возможность монтажа оборудования и прокладка сигнальных кабелей на боковых стенках шкафов согласовываются с Заказчиком.

В шкафах должны быть предусмотрены:

- концевые выключатели состояния дверей шкафа;
- сигналы состояния блоков питания (БП), активного сетевого оборудования, сигнализацию барьерных и релейных плат.

Данные сигналы являются системными и не учтены в сводной таблице количества входных/выходных сигналов. В предложении поставщика должны быть отдельно указаны данные сигналы и предполагаемое для их обеспечения оборудование.

Силовые кабели должны входить в шкафы с нижней стороны через соответствующие узлы подключения кабелей, при этом внутренние провода распределения питания должны идти в отдельных сигнальных каналах. Сигнальные кабели должны входить в шкафы с нижней стороны через соответствующие узлы подключения.

Должно быть предусмотрено освещение внутри шкафов.

На внутренних сторонах дверей, с каждой стороны шкафа, предусмотреть карманы для размещения документации.

На наружных сторонах шкафов, предусмотреть легко читаемую табличку с маркировкой шкафа, согласно проекту.

Окончательная компоновка шкафа и конструкция утверждаются Заказчиком.

В шкафах должно быть предусмотрено подключение линий питания полевых приборов, требующих независимого питания 24 В постоянного тока или 220 В переменного тока.

Все кабели, клеммники должны быть промаркированы. Сигнальные линии и линии для питания КИП должны коммутироваться через клеммы с размыкателем или предохранителем.

Кроссовые шкафы должны быть оборудованы клеммниками с ножевыми расцепителями.

Все полевые линии (сигнальные и линии питания) должны иметь защиту от короткого замыкания. Защита может выполняться промежуточным реле, предохранителем, или автоматическим выключателем. Короткое замыкание на любой линии не должно приводить к перегрузке источника питания и обесточиванию других линий.

Шкафы должны состоять из полевой части и контроллерной части.

Полевая часть (полевой клеммник) строится в соответствии с кабельным журналом, т.е. является отображением полевых кабелей. Все полевые кабели и все жилы полевых

кабелей подключаются к клеммам строго последовательно. Перекрестное подключение жил разных кабелей не допускается.

Контроллерная часть кросса строиться в соответствии с модулями ввода/вывода системы. Все каналы всех модулей ввода/вывода последовательно подключаются к клеммам или терминальным устройствам контроллерной части кросса.

Электропитание разделительных реле должно выполняться по резервированным линиям.

Для подключения соответствующей полевой линии к соответствующему входу системы используются кроссировочные линии.

Во всех вновь устанавливаемых шкафах и панелях, шасси контроллеров АСУТП необходимо предусматривать не менее 20% свободного места для размещения оборудования. При использовании существующих корпусов шкафов данное требование выполнять при такой возможности.

Шкафы с сетевым оборудованием должны соответствовать следующим требованиям:

- в шкафах предусмотреть размещение сетевого оборудования;
- двустороннего, напольного монтажа, с нижним подводом кабелей;
- с углом открывания дверей не менее 170˚;
- поставляться в сборе;
- состояние открытия дверей шкафов должно регистрироваться в АСУТП;
- иметь встроенный вентилятор, внутреннее освещение и розетку 220В;
- иметь датчик контроля температуры внутри шкафа с регистрацией показаний в АСУТП;
- при необходимости иметь однорядные клеммники с ножевыми размыкателями или предохранительными вставками;
- с шиной центрального заземления;
- с шиной информационного заземления.

Искробезопасные и искроопасные цепи должны быть разделены и прокладываться раздельными кабелями или проводами в разных коробах (лотках, стойках, вводах).

Так как каждый шкаф является низковольтным комплектным устройством (НКУ) распределения, управления, измерения, сигнализации и защиты, то он должен быть укомплектован паспортом на изделие. В паспорте должно быть определено соответствие НКУ требованиям ГОСТ IEC 61439-1-2013, ГОСТ 30804.6.2-2013, ГОСТ Р 51317.6.4-2009.

Требования к техническому обеспечению АРМ ОТ.

АРМ должны быть созданы на базе персонального компьютера промышленного исполнения и включать в себя:

- четыре цветных графических дисплея с размером экрана не менее 27”, с возможности вывода видеоинформации до 6 графических дисплеев (для возможности дальнейшей модернизации АРМ);
- системный блок с улучшенным охлаждением и защитой от пыли, размещаемый в нише существующей мебели;
- наличие дублированных жестких дисков с RAID-1 контроллером (выделенная плата);
- манипулятор типа «мышь»;
- универсальную алфавитно-цифровую клавиатуру (рус./лат.);
- колонки для вывода звуковой информации.

Требования к техническому обеспечению ИС.

ИС должны быть созданы на базе персонального компьютера промышленного исполнения и включать в себя:

- два цветных графических дисплея с размером экрана не менее 27”;
- системный блок с улучшенным охлаждением и защитой от пыли, размещаемый в нише существующей мебели;
- наличие дублированных жестких дисков с RAID-1 контроллером (выделенная плата);
- манипулятор типа «мышь»;
- универсальную алфавитно-цифровую клавиатуру (рус./лат.);
- колонки для вывода звуковой информации.

Кроме того, ИС должны иметь средства для сохранения конфигурации системы на сменные носители.

Требования к техническому обеспечению локальных АРМ ОТ.

Локальные АРМ ОТ должны быть созданы на базе персонального компьютера промышленного исполнения и каждая должна включать в себя:

- один цветной графический дисплей с размером экрана не менее 27”;
- манипулятор типа «мышь»;
- универсальную алфавитно-цифровую клавиатуру (рус./лат.)
- колонки для вывода звуковой информации.

Все АРМ должны работать независимо друг от друга, то есть выход из строя одной или нескольких станций не должен влиять на работу других.

Требования к интерфейсу оператора указаны в **Приложении А** данных Технических требований.

Требования к сетевому оборудованию.

Обмен данными между контроллерами, АРМ ОТ, ИС должен выполняться по высокоскоростной резервированной линии связи со скоростью передачи не менее 100 Мбит/с.

Кроме того, Система управления должна обеспечивать передачу данных в информационную сеть предприятия средствами OPC. В состав поставки включить лицензии для организации передачи данных в заводскую сеть с помощью OPC, предусмотреть достаточность лицензий OPC для интеграции. Объем передаваемой информации принять по существующему – точное количество будет указано Заказчиком.

Сервер OPC должен применяться для хранения истории, передачи данных в общезаводскую сеть по OPC протоколу. Новое серверное оборудование должно быть рассчитано на не мене 5000 сигналов по цифровым протоколам. Серверное оборудование должно обладать достаточной мощностью для работы оборудования 1 и 2 очереди ГТУ-ТЭС, поддерживать протокол передачи данных для внешних САУ: OPC DA/UA, все необходимые лицензии, способным обрабатывать как железные сигналы от контроллеров, так и цифровые сигналы с запасом по мощности для объектов второй очереди и будущих технических решений. Отклик на действия оператора – не более 1 секунды.

Построение резервированных каналов передачи данных должно исключать нарушение нормальной работы системы управления при единичном отказе любого сетевого оборудования или обрыве одного кабеля связи. Электропитание активного сетевого оборудования должно быть резервировано.

Все активное сетевое оборудование должно быть промышленного исполнения (с улучшенным охлаждением). Система должна постоянно выполнять диагностику сетевого оборудования и при обнаружении неисправности формировать сообщение оператору и инженеру АСУТП.

Требования к электроснабжению.

Схема электропитания АСУТП должна соответствовать требованиям ПУЭ для особой группы 1-й категории электроснабжения.

В рамках поставки нового оборудования должна быть сохранена существующая схема питания.

Требования к заземлению.

Все внешние элементы технических средств АСУ, находящиеся под напряжением, металлоконструкции для установки электрооборудования должны иметь защиту от

случайного прикосновения человека, а сами технические средства иметь защитное заземление в соответствии с требованиями «Правил устройства электроустановок», и ГОСТ 12.1.030-81 ССБТ «Защитное заземление, зануление».

Для микропроцессорного контроллера будет предусмотрен отдельный функциональный контур заземления, необходимый для устойчивой работы оборудования и защиты от помех общего вида (блуждающих токов, наводок от токов замыкания на землю и т.п.) с сопротивлением заземлителя растеканию тока 4 Ом. Наличие контура обеспечивается Заказчиком по рекомендациям Поставщика.

Для подключения к контуру функционального заземления щитов контроллера использовать одножильные изолированные провода.

Экраны кабелей должны быть подключены с одной стороны к контуру функционального заземления расположенному в щите, если иное не предписывается фирмой-изготовителем оборудования.

4.3.2 Требования к программному обеспечению

Вместе с техническими средствами системы должны быть поставлены лицензионные стандартные пакеты программного обеспечения.

Программное обеспечение должно быть достаточным для реализации всех функций системы управления и иметь средства для организации всех требуемых процессов обработки данных.

Кроме того, в комплект поставки должно быть включено следующее отечественное программное обеспечение (ПО):

- антивирусное ПО, протестированное на совместимость с ПО АСУТП и рекомендованное производителем (поставщиком) средств АСУТП;
- ПО для создания проектов, конфигурирования системы на инженерной станции;
- ПО для создания мнемосхем (видеоэкранов) на инженерной станции;
- ПО для автодокументирования базы данных и алгоритмов системы;
- ПО для формирования рапортов и отчетов;
- ПО для передачи данных на верхний уровень (в заводскую сеть);
- ПО для резервного копирования данных и создания образов;

Программное обеспечение (ПО) должно удовлетворять следующим требованиям:

- модульность построения прикладного ПО, подразумевающая независимую разработку и отладку отдельных модулей ПО с последующей их компоновкой в программе системы;
- открытость ПО, позволяющая корректировать и расширять ПО при появлении производственной необходимости;

– гибкость и возможность настройки ПО системы в соответствии с условиями производственных задач.

Программное обеспечение должно обеспечивать выполнение следующих задач и поддерживать языки программирования, удовлетворяющие требованиям стандарта IEC 61131-3. ГОСТ Р МЭК 61131-3-2016:

- разработку программ, функций и функциональных блоков;
- использование разработанных библиотечных функций и функциональных блоков;
- графическое конфигурирование входных и выходных модулей и точек;
- конфигурирование регистрации последовательности событий;
- регулировать доступ к программам средствами администрирования;
- отлаживать программу, используя функции эмуляции;
- печать таблиц данных, листингов программы;
- использование средств диагностики для выявления отказов аппаратных средств;
- экспортирование данных в файлы редактируемых форматов.

ПО должно выполнять учет времени наработки технологического оборудования (насосов и т.п.).

4.3.3 Требования к метрологическому обеспечению

При разработке системы управления должна быть предусмотрена возможность контроля метрологических характеристик ее измерительных каналов.

Метрологическое обеспечение измерительных систем должны соответствовать ГОСТ Р 8.596-2002. ГСИ. "Метрологическое обеспечение измерительных систем. Основные положения".

Метрологическое обеспечение АСУТП должно отвечать требованиям:

- МИ 2440-97 «Государственная система обеспечения единства измерений. Методы экспериментального определения и контроля характеристик погрешности измерительных систем и измерительных комплексов»;
- МИ 2439-97 «Метрологические характеристики измерительных систем. Номенклатура. Принципы регламентации, определения и контроля»;
- Федеральных норм и правил в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств» (Приказ №533 от 15 декабря 2020г., раздел 6.6);
- Федеральный закон от 26.06.2008 №102-ФЗ «Об обеспечении единства измерений» (с изменениями на 13 июля 2015 г.).

Система должна быть поверена в соответствии с методикой, предусмотренной для нее при утверждении типа СИ. Должна быть проведена поверка (калибровка) измерительных каналов ПТК АСУТП на площадке Заказчика, по результатам которой должны быть оформлены соответствующие протоколы и получено свидетельство о поверке (калибровке).

Свидетельство о поверке (калибровке) измерительных каналов АСУТП предоставляется поставщиком системы на этапе передачи в опытно-промышленную эксплуатацию.

Для проведения поверки аналоговых модулей ввода-вывода (AI и AO) при проектировании предусмотреть наличие специально выделенных и сконфигурированных слотов (поверочные слоты). Количество слотов должно соответствовать количеству уникальных типов аналоговых входных и аналоговых выходных модулей, применяемых в поставляемой системе. Слоты должны быть расположены в непосредственной близости друг от друга и сконфигурированы под полное штатное количество каналов соответствующих типов модулей. Должна быть обеспечена возможность подключения ко всем каналам модулей. Результаты измерений должны отображаться на специально разработанной мнемосхеме или в сервисном ПО системы в тех же единицах измерения, которые указаны в описании типа СИ поставляемой системы.

Значения контролируемых параметров (технологического процесса, технологического оборудования) должны быть выражены в соответствии с ГОСТ 8.417-2002 "ГСИ. Единицы величин".

Средства измерения (СИ), входящие в систему контроля и управления должны иметь сертификат об утверждении типа СИ, описание типа СИ, методику поверки.

В спецификацию оборудования АСУТП должны быть включены специальные технические и программные средства для калибровки измерительных каналов.

Все методики измерения, используемые в сфере государственного метрологического контроля и надзора, должны быть аттестованы.

При поверке каналов Системы должна быть предоставлена возможность доступа ко всем элементам Системы для подключения образцовых приборов (калибраторов).

Все метрологические характеристики измерительных и управляющих модулей должны быть представлены фирмой-изготовителем в документации на технические и программные средства. Пределы допускаемых значений погрешности измерительных каналов не должны превышать норм Технологического Регламента.

Относительная погрешность отдельного модуля ввода аналоговых сигналов без учета первичного датчика, линии связи, преобразователей не должна превышать ±0.5%.

Межповерочный интервал поставляемой Системы должен составлять не менее 3 лет.

Дополнительная погрешность, вызванная изменением температуры воздуха в пределах рабочего диапазона не должна превышать половины основной погрешности на каждые 10°С.

Оборудование системы должно иметь необходимые сертификаты органов стандартизации (Федеральное Агентство по техническому регулированию и метрологии) России (сертификаты об утверждении типа СИ, описания типа СИ, методики поверки/калибровки) и действующие свидетельства о поверке/калибровки на момент ввода АСУТП в эксплуатацию. На момент поставки Система должна иметь действующие свидетельства о поверке. Остаток межповерочного интервала на момент ввода должен составлять не менее 2/3 значения, установленного при утверждении этого типа систем.

4.3.4 Требования к информационному обеспечению

Информационное обеспечение должно быть достаточным по объему и содержанию для оперативной и достоверной оценки состояния технологического оборудования, режимов его работы, оценки и функционирования подсистем АСУТП, распознавания отказов.

Информационное обеспечение должно включать:

- информационные массивы, включая входную аналоговую и дискретную информацию, результаты расчета и наиболее важные промежуточные результаты, нормативно-справочную информацию;
- систему ведения, редактирования и формирования базы данных;
- систему классификации и кодирования информации, кодовые словари и справочники;
- формы выходных документов (видеограммы ведомостей и т.п.);
- программные средства передачи информации между компонентами АСУТП и в смежные информационные системы. По способу хранения, информационные массивы должны быть организованы в виде ОЗУ-резидентных массивов и файлов на внешних запоминающих устройствах в соответствии с требованиями файловой системы ОС.

Информационное обеспечение АСУТП должно предусматривать возможность расширения информационных массивов с учетом перспектив развития.

Технологическая информация должна быть представлена оператору следующими способами:

- отображением информации о состоянии оборудования рабочих сред, запорной и регулирующей арматуры на дисплеях АРМ ОТ;
- включением световой индикации на дисплеях (выделением цветов, мерцанием и т.п.) и звуковой сигнализации (предупредительной и аварийной) средствами АСУТП;

– печатью по вызову протоколов работы защит, логических задач, команд оператора, изменения величин параметров и т.д.,
– периодической печатью (по вызову) показателей работы оборудования (средствами ПТК АСУТП для оперативных функций и для расчетных задач).

Применяемые в выходных документах и на устройствах отображения информации термины и сокращения должны быть общепринятыми в отрасли.

Принятая система идентификации должна применяться во всей документации на АСУТП, включая программную.

В основу построения информационного обеспечения АСУТП должен быть положен принцип однократного ввода и многократного использования информации внутри системы.

Для придания юридической силы документам, выдаваемым АСУТП, должны соблюдаться следующие требования:

– каждая ведомость или страница ведомости должны содержать наименование объекта контроля, идентификационный номер оборудования, информация по которому представлена в документе, дату и время выдачи документа, реквизиты и место для подписи ответственного лица (дежурного старшего оператора);
– на каждой странице должен проставляться номер страницы и общее число страниц в документе;
– при недостоверности значений и сигналов в ведомостях должно печататься соответствующее сообщение.

4.3.5 Требования к математическому обеспечению

Математическое обеспечение системы управления должно реализовывать все перечисленные выше функции и базироваться на использовании универсальных алгоритмов решения задач.

Используемые алгоритмы по возможности должны быть унифицированы и разрабатываться по модульному принципу.

Математическое обеспечение АСУТП должно обеспечивать реализацию основных функций:

- первичной обработки сигналов (контроль достоверности всех сигналов, их фильтрацию, масштабирование);
- обработки, накопления, усреднения, интегрирования;
- программно-логического непрерывного контроля.

Математическое обеспечение АСУТП должно позволять выполнять, как минимум следующие операции:

- сложение, вычитание, деление, умножение;
- извлечение квадратного корня, возведение в степень;
- интегрирование и дифференцирование;

- операции с логарифмами;
- логические операции И, ИЛИ, НЕ;
- действия с селекторами сигналов, таймерами, триггерами, звеньями задержки;
- PID управление;
- математические вычисления с плавающей запятой;
- автоматический/ручной режимы работы для регуляторов;
- функции изменения сигнала по линейному закону;
- опережение-запаздывание, линия задержки сигнала.

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ АСУТП

Разработка АСУТП осуществляется в соответствии с ГОСТ 34.601-90 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» и ввод в действие АСУТП осуществляется в соответствии с требованиями СП 77.13330-2016 «Системы автоматизации».

Разработчик АСУТП Объекта осуществляет поставку оборудования, выполнение техно-рабочего проекта, пуско-наладочных (ПНР) и инжиниринговых работ - далее Поставщик.

5.1 Выбор поставщика АСУТП

В Технико-коммерческом предложении (ТКП) от возможных поставщиков необходимо учесть настоящие «Технические требования на АСУТП.

Техническое предложение (ТП) должно содержать следующие позиции и условия:

- пояснительная записка с кратким описанием (на русском языке) предлагаемого оборудования, структуры построения, сетей обмена информацией, системы бесперебойного электропитания и т.д.;
- структурную схему построения предлагаемой системы управления с указанием интерфейсов связи между компонентами системы и используемого программного обеспечения;
- структурную схему электропитания КТС АСУТП (на базе предлагаемого оборудования);
- разработка комплекта документов, в виде, предусмотренном ГОСТ 34.201-2020 («Виды, комплектность и обозначение документов при создании автоматизированных систем»)—Перечень требуемых документов представлен в **Приложении Е** данных ТТ. Документация должна быть оформлена по ГОСТ;
- работы и перечень отчётной документации, связанные с использованием системы должны соответствовать ГОСТ Р 59792-2021 ИТ «Виды испытаний автоматизированных систем».. Перечень требуемой отчётной документации представлен в **Приложении Ж** данных ТТ;
- при наличии в составе системы оборудования третьих фирм должны быть учтены программное обеспечение и адаптеры для конфигурирования и настройки такого оборудования;
- Сертификаты Технического регламента таможенного союза на все поставляемое оборудование АСУТП;
- должны быть актуальные решения, выпущенные для общей продажи, обеспечивающие полную аппаратурную совместимость всех используемых компонентов;
- срок эксплуатации оборудования;

- полный (подробный) перечень (спецификация) поставляемого оборудования и услуг (выполняемых работ) с указанием инжиниринговых, строительно-монтажных, шеф-монтажных и пуско-наладочных работ. Перечень (спецификация) поставляемого оборудования должен содержать наименование/краткое описание оборудования на русском языке;
- оборудование в спецификации должно быть разделено по следующим принципам:
    - место размещения (операторная, контроллерная/аппаратная и т.д.);
    - по шкафам (например, контроллерный, кроссовый, Сетевой, Серверный и т.д.);
    - аппаратное, программное и лицензионное обеспечение должно быть привязано к каждой конкретной рабочей станции.
- при отсутствии системы лицензирования на использование количества тегов, указывать максимально возможное количество сигналов, которое система способна обрабатывать;
- перечень всех лицензий (попозиционно), необходимых для использования всех программных продуктов АСУТП;
- сведения о месте сборки и тестирования поставляемого оборудования;
- таблицу необходимого и предложенного количества входов/выходов, включая реле и барьеры искрозащиты;
- схему прохождения сигналов от входного клеммника до центрального процессора, включая реле и барьеры искрозащиты, терминальные панели (с указанием количества и канальности элементов/модулей);
- сертификаты и Разрешения Российской Федерации на применение предлагаемого оборудования;
- для интеграторов обязательно наличие подтверждения вендора на право продажи и гарантийного сопровождения предлагаемого оборудования.

ТКП должно включать:

- оборудование АСУТП (контроллеры, АРМ, система бесперебойного электропитания, оборудование связи и коммуникации, кабельная продукция и т.д.);
- выполнение проектных работ. Прохождение экспертизы промышленной безопасности ТРП. Предоставление Заказчику положительного заключения экспертизы промышленной безопасности ТРП (**Приложение Е** данных ТТ);
- работы по инжинирингу (**Приложение З** данных ТТ);
- пуско-наладочные работы по комплексу технических средств системы, включая систему электропитания (**Приложение И** данных ТТ);
- Запасные изделия и принадлежности (10 % от каждого применяемого компонента, но не менее 1 шт.), включая 1 системный блок, 1 монитор для АРМ. Под

компонентами подразумевается активное оборудование, такое как: контроллер, модуль связи, модуль интерфейсный, источник питания, модуль ввода-вывода, устройства АВР, коммутатор, барьер искрозащиты, реле, преобразователь интерфейса и т.п. Под компонентами не подразумеваются монтажные изделия, компоненты шкафного, кроссового оборудования, кабельная продукция, изделия и материалы.

- калибраторы и другое образцовое оборудование, необходимое для поверки системы;
- hart-коммуникатор;
- сроки поставки оборудования на площадку Заказчика;
- условия поставки;
- гарантийные обязательства (не менее 24 месяцев, с момента передачи системы в промышленную эксплуатацию или 36 месяцев от даты отгрузки);
- комплектацию операторной мебели (консоли, тумбы для принтеров, кресла и т.п.).

Срок действия предложения - 12 месяцев.

Требования к поставке оборудования АСУТП указаны в **Приложении В** данных Технических требований.

5.2 Документация

Документация на программно-технический комплекс должна быть представлена на русском языке и оформлена согласно стандартным формам.

Изменения, внесенные в ходе приемки, должны быть отражены в общей документации.

В процессе выполнения контракта Поставщиком должны выдаваться следующие документы, которые подлежат согласованию Заказчиком (дается не полный перечень):

- график выполнения контракта с указанием ключевых дат;
- структурная схема с указанием информационных потоков и протоколов обмена;
- характеристики шкафов и пультов;
- требования к электроснабжению и заземлению;
- электрические схемы шкафов;
- чертежи клеммников;
- функциональные спецификации конфигурирования;
- базовые мнемосхемы;
- базовые группы параметров;
- баланс мощности;
- баланс тепловыделения;

В состав окончательной документации входят (перечень не исчерпывающий):

- комплектная документация системы;
- инструкция по монтажу;
- инструкция по эксплуатации, инструкция по техобслуживанию;
- описание и технические данные системы;
- спецификация поставляемого оборудования;
- описание программных средств, документы, переданные на одобрение, распечатки возможных конфигураций, выводимые копии с экрана;
- методики метрологической аттестации;
- инструкция по заземлению.

Содержание окончательной документации должно быть согласовано Заказчиком.

Перечень документации, необходимой для конфигурирования АСУТП указан в **Приложении Б** данных Технических требований.

Документация должна быть выполнена по ГОСТ 34.201-2020, ГОСТ 34.602-2020.

В процессе создания проект, либо отдельные части проекта, должны предъявляться Заказчику на рассмотрение и согласование в бумажном или электронном виде в формате PDF (*.pdf), в формате электронных таблиц и текстовых документов.

Каждый отдельный документ должен содержать фамилии и подписи ответственных лиц, разработавших, проверивших и утвердивших документ (при направлении документации, как в бумажном, так и в электронном виде).

Документация предоставляется в электронном виде и на бумажном носителе в 4 экз.

5.3 Проверка и испытания АСУТП

Система сдается в опытно-промышленную эксплуатацию по акту. По результатам опытно-промышленной эксплуатации составляется совместный акт приемки системы в постоянную эксплуатацию. Состав приемной комиссии определяется Заказчиком.

Приемка АСУТП состоит из нескольких этапов (см. ГОСТ 34.601-90, СП77.13330-2016 «Системы автоматизации», ГОСТ Р 59792-2021 ИТ «Виды испытаний автоматизированных систем»):

- пуско-наладочные работы;
- предварительные испытания;
- опытная эксплуатация;
- приемочные испытания;
- выполнение работ в соответствии с гарантийными обязательствами.

На этапе «Пусконаладочные работы» проводят автономную наладку технических и программных средств, загрузку информации в базу данных и проверку системы ее ведения, комплексную наладку всей системы.

Пусконаладочные работы по системам автоматизации (далее - пусконаладочные работы) должны быть выполнены таким образом, чтобы была обеспечена реализация технических решений по автоматизации технологического процесса, принятых в проектной и рабочей документации;

Пусконаладочные работы по системам автоматизации проводят в соответствии с решениями и нормами, предусмотренными проектной и рабочей документацией, технологическим регламентом (производственной инструкцией), эксплуатационной документацией на технические и программные средства систем автоматизации предприятий-изготовителей и разработчиков, требованиями федеральных норм и правил в области промышленной безопасности;

Пусконаладочные работы по системам автоматизации проводят в три стадии:

- I стадия - подготовительные работы;
- II стадия - автономная наладка систем автоматизации (вхолостую);
- III стадия - комплексная наладка систем автоматизации (под нагрузкой).

На этапе «Предварительные испытания» осуществляют:

- испытания программно-технического комплекса в соответствии с программой и методикой предварительных испытаний; устранение неисправностей и внесение изменений в документацию АСУТП, в том числе эксплуатационную, в соответствии с протоколом испытаний;
- оформление акта о приемке АСУТП в опытную эксплуатацию.

На этапе «Опытная эксплуатация» проводят:

- опытную эксплуатацию программно-технического комплекса;
- анализ результатов опытной эксплуатации;
- доработку (при необходимости) программного обеспечения;
- дополнительную наладку (при необходимости) технических средств программно-технического комплекса;
- оформление акта о завершении опытной эксплуатации.

Во время опытной эксплуатации системы ведется рабочий журнал, в который заносятся сведения о результатах наблюдения за правильностью ее функционирования, об отказах, сбоях, аварийных ситуациях, корректировках технической документации.

На этапе «Приемочные испытания» проводят:

- испытания на соответствии техническому заданию в соответствии с программой и методикой приемочных испытаний;
- анализ результатов испытаний программно-технического комплекса и устранение недостатков, выявленных при испытаниях;
- оформление акта о приемке АСУТП в промышленную эксплуатацию.

Результаты приемочных испытаний системы должны быть оформлены актом, утверждаемым в установленном порядке. Акт должен содержать заключение о соответствии системы требованиям Технического задания и решение комиссии о приемке системы в промышленную эксплуатацию.

На этапе «Выполнение работ в соответствии с гарантийными обязательствами» осуществляются работы по устранению недостатков, выявленных, при эксплуатации АСУТП в течение установленных гарантийных сроков, внесению необходимых изменений в документацию на АСУТП.

При проведении приемки, комиссии предъявляется АСУТП в полном комплекте:

- комплекс технических средств, смонтированный, соединенный, налаженный и скомплексированный, подготовленный к эксплуатации обученным персоналом;
- проектную документацию со всеми изменениями и дополнениями;
- эксплуатационную документацию необходимую для освоения АСУТП и ее нормальной эксплуатации;
- программное обеспечение в виде загруженных модулей рабочего ПО, его копий на внешних носителях и программная документация;
- технические описания комплекса технических средств;
- ЗИП, приборы, устройства и стенды, необходимые для регламентных работ, проверки работоспособности комплекса технических средств и метрологического контроля.

Перечень отчетных документов по приемке и монтажу АСУТП приведен в **Приложении Ж.**

6 НОРМАТИВНЫЕ ДОКУМЕНТЫ

При создании системы управления необходимо руководствоваться следующими нормативными документами:

№ П/П	ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ
1	2
1	ГОСТ 34.602-2020. Техническое задание на создание АС
2	ГОСТ Р 59793-2021. Автоматизированные системы. Стадии создания
3	ГОСТ 34.201-2020. Виды, комплектность и обозначение документов при создании автоматизированных систем
4	ГОСТ 24.104-2023. Автоматизированные системы управления. Общие требования
5	ГОСТ 24.701-86. ЕСС АСУ. Надежность АСУ. Основные положения
6	ГОСТ 21958-76. Общие эргономические требования к расположению рабочих мест
7	ГОСТ 12.1.030-81. ССБТ. Защитное заземление, зануление
8	ГОСТ 12.1.003-83. ССБТ. Шум. Общие требования безопасности
9	ГОСТ Р 59792-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем.
10	ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»
11	ПУЭ. Правила устройства электроустановок. Актуальное издание.
12	Федеральные нормы и правила в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств» утвержденные Приказом №533 Федеральной службы по экологическому, технологическому и атомному надзору от 15 декабря 2020 года
13	ГОСТ Р МЭК 61508-2-2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»
14	ГОСТ 27.301-95 «Надежность в технике. Расчет надежности. Основные положения»
15	СП 77.13330-2016 «Системы автоматизации»
16	ГОСТ Р 8.596-2002. ГСИ. Метрологическое обеспечение измерительных систем. Основные положения.
17	МИ 2439-97. ГСИ. Метрологические характеристики измерительных систем. Номенклатура. Принципы регламентации, определения и контроля. МИ 2440-97. ГСИ. Методы экспериментального определения и контроля характеристик погрешности измерительных каналов измерительных систем и измерительных комплексов.
18	МИ 2440-97. Рекомендация. Государственная система обеспечения единства измерений. Методы экспериментального определения и контроля характеристик погрешности измерительных каналов измерительных систем и измерительных комплексов.
19	Положение Компании «Информационная безопасность. Автоматизированные системы управления технологическими процессами» № П3-11 Р-0012.
20	Федеральный закон от 26 июня 2008 г. N 102-ФЗ «Об обеспечении единства измерений» (с изменениями и дополнениями).
21	ГОСТ Р 59795-2021 «АС. Требования к содержанию документов»

№ П/П	ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ
1	2
22	ГОСТ Р 58604-2019 «Тепловые электрические станции. Автоматизированные системы управления технологическими процессами. Условия создания. Нормы и требования.»
23	РД 153-34.1-35.137-2003. «Технические требования к подсистеме технологических защит, выполненных на базе микропроцессорной техники»
24	РД 153-34.1-35.145-2003. «Технические требования к функции ПТК АСУ ТП ТЭС "Сбор и первичная обработка информации"
25	Приказ № 1070 Минэнерго России от 04.10.2022 «Об утверждении Правил технической эксплуатации электрических станций и сетей Российской Федерации»
26	Приказ № 796 Минэнерго России от 22.09.2020 «Об утверждении Правил работы с персоналом в организациях электроэнергетики Российской Федерации»
27	Приказ ФСТЭК РФ от 14.03.2014 № 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». (Федеральный закон от 26.07.2017 № 187-ФЗ)
28	Приказ ФСТЭК РФ от 25 декабря 2017г. №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

7 ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АВЗ	антивирусная защита
АВР	автоматическое включение резерва
АРМ	автоматизированное рабочее место
АСУТП	автоматизированная система управления технологическими процессами
БП	блок питания
ВОЛС	волоконно-оптическая линия связи
ЗИП	запасные инструменты и приборы
ИБП	источник бесперебойного питания
ИС	инженерная станция
КИПиА	контрольно-измерительные приборы и автоматика
КТС	комплекс технических средств
МПК	микропроцессорный контроллер
НПЗ	нефтеперерабатывающий завод
ОПО	опасный производственный объект
ОТ	оператор-технолог
ПО	программное обеспечение
ПТК	программно-технический комплекс
СИ	средство измерения
ССУ	специальная система управления
ТТ	технические требования
УСО	устройство связи с объектом
ШРП	шкаф распределения питания

Приложение А
Требования к интерфейсу оператора

А.1 Требования к размещению и компоновке рабочих мест

А.1.1 Система должна включать автоматизированные рабочие места:

- девять АРМ ОТ;
- восемь локальных АРМ ОТ;
- одна инженерная станция (ИС);
- одна ИС резервного копирования;

Точное количество ИС, станций копирования или иных АРМ определяется поставщиком по согласованию с Заказчиком на этапе технических предложений.

А.1.2 Рабочие места должны быть укомплектованы

- АРМ ОТ, ИС , ИС резервного копирования - двумя жидкокристаллическими мониторами;
- Локальные АРМ ОТ – одним жидкокристаллическим монитором.

А.1.3 В состав рабочих мест операторов должны входить принтеры для распечатки рапортов, сообщений о ходе технологического процесса.

А.1.4 Управление технологическим процессом должно производиться с помощью манипулятора «мышь» и универсальной алфавитно-цифровой клавиатуры (рус./лат.).

А.1.5 Пульт управления должен быть построен на модульном принципе – на каждое рабочее место должен быть предусмотрен свой модуль (консоль). Должны быть предусмотрены модули для размещения АРМ ОТ, ИС, тумбы для принтеров.

А.2 Общие требования

А.2.1 Должно быть обеспечено цветовое единство интерьера и средств вычислительной техники.

А.2.2 Основным средством представления информации оператору должен являться цветной графический монитор.

А.2.3 Технологические сообщения оператору должны быть на русском языке, системные сообщения могут быть на английском и русском языках.

А.2.4 Для операторского интерфейса должна быть предусмотрена система защиты от несанкционированного доступа к изменяемым параметрам Системы.

А.3 Структура операторского интерфейса

А.3.1 Взаимодействие оператора с Системой должно обеспечиваться иерархической системой видеокадров. Каждый видеокадр должен содержать:

- рабочую область, содержащую мнемосхему процесса;
- кнопки для вызова требуемых мнемосхем в верхней части экрана;
- сигнальную строку в нижней части экрана.

А.3.2 Мнемосхемы процесса должны в максимальной степени отражать структуру объекта и его текущее состояние, а именно:

- состав технологического оборудования;
- динамику изменения состояния процесса;
- численные значения параметров процесса;
- состояние отсечных клапанов и агрегатов.

А.3.3 По степени детализации отображения информации операторский интерфейс должен включать следующие виды мнемосхем:

- детальные мнемосхемы;
- групповые мнемосхемы;
- обзорные мнемосхемы.

А.3.4 Операторский интерфейс должен включать стандартные видеограммы:

- тренды реального времени;
- исторические тренды;
- экраны настройки регуляторов;
- экраны аварийной и предупредительной сигнализации (текущие и исторические);
- экраны формирования отчетов;
- экран диагностики Системы;
- экран парольной защиты;
- экран блокировок.

А.3.5 Тренды должны обеспечивать отображение текущих (в реальном времени) и зарегистрированных (история процесса) значений параметров в виде временных графиков. Исторические тренды должны быть доступны для просмотра и печати в виде графиков.

А.3.6 Экран аварийной и предупредительной сигнализации должен содержать в хронологическом порядке перечень сообщений об отклонениях контролируемых параметров.

А.3.7 Экран формирования отчетов должен содержать меню с перечнем формируемых отчетов. Допускается формирование отчетов на сервере БД верхнего уровня. Перечень и форма отчетов определяется на этапе выполнения технорабочего проекта.

А.3.8 Графическое содержание мнемосхем и видеограмм определяется на этапе разработки проекта.

А.3.9 На экране, обеспечивающем оперативный контроль за несанкционированными изменениями значений уставок сигнализации и блокировок, отображается информация о фактических значениях уставок сигнализации и блокировок технологических параметров и значения уставок сигнализации и блокировок технологических параметров согласно технологического регламента (проектных).

В случае несоответствия значений срабатывает световая сигнализация.

А.4 Отображение информации на мнемосхемах

А.4.1 Информация о значениях параметров процесса должна отображаться в виде численных значений. Параметры и их значения должны отображаться следующим образом:

- аналоговые сигналы должны иметь поле с наименованием позиции датчика, поле численного значения и единиц измерения;
- дискретные сигналы должны иметь поле с наименованием позиции датчика.

А.4.2 Наименование позиций аналоговых и дискретных сигналов на мнемосхемах должно соответствовать таблице входных/выходных сигналов объекта.

А.4.3 Для сигнализации отклонений аналоговых параметров от заданных пределов должно применяться цветовое кодирование, настраиваемое по согласованию с Пользователем системы (Заказчиком) при конфигурировании.

А.4.4 При получении сигналов от датчиков-сигнализаторов должно применяться цветовое кодирование наименования позиции, соответствующее отклонению параметра от уставки:

- при значение параметра ниже предупредительной уставки;
- при значение параметра ниже аварийной уставки;
- при значение параметра выше предупредительной уставки;
- при значение параметра выше аварийной уставки.

Цвет и способ сигнализации настраиваются при конфигурировании.

А.4.5 Цветовое кодирование состояния запорной арматуры.

Цветовое кодирование состояния запорной арматуры предлагается Разработчиком АСУТП и согласовывается с Заказчиком.

А.4.6 Цветовое кодирование состояния насосных агрегатов, компрессоров, вентиляторов должно быть следующим:

Цветовое кодирование состояния насосных агрегатов, компрессоров, вентиляторов и т.п. предлагается Разработчиком АСУТП и согласовывается с Заказчиком.

А.4.7 Взаимодействие оператора с процессом при выполнении функций управления должно осуществляться с помощью манипулятора «мышь» и клавиатуры.

А.5 Сигнализация

А.5.1 В Системе должна быть предусмотрена предаварийная и предупредительная сигнализация при отклонениях технологического процесса и нарушениях в работе оборудования. Сигнализация должна формироваться при возникновении следующих условий:

- выход аналогового параметра за границы уставок;
- срабатывание дискретных сигнализаторов;

- срабатывание блокировок с фиксацией первопричины останова оборудования;
- аварийный останов технологического оборудования (насосы, нагревательные печи, компрессоры, вентиляторы);
- отказ оборудования Системы;
- отключение внешнего электропитания и переход на резервное электропитание.

А.5.2 Сигнализация должна производиться:

- миганием графического отображения технологического оборудования соответствующим цветом;
- включением звукового сигнала;
- записью причины и времени срабатывания сигнализации в журнал сигнализации, а также времени квитирования сигналов сигнализации;
- появлением на экране сообщения с причиной сигнализации.

Текстовое оповещение о событиях (технологическая сигнализация, системное сообщение и т.п.) должно отображаться в специальной строке графического интерфейса Системы.

А.5.3 Действие звуковой сигнализации и мигание изображения параметра (оборудования) должно продолжаться до момента квитирования (подтверждения) сообщения оператором. Цветовая индикация отклонений на мнемосхеме и отображение отклонений на экране текущей аварийной сигнализации должны сохраняться до тех пор, пока значение параметра не войдет в норму.

А.5.4 При срабатывании аварийно-предупредительной сигнализации должна быть предусмотрена возможность вызова на экран (с помощью манипулятора «мышь») соответствующей мнемосхемы технологического процесса и/или лицевой панели ПИД-регулятора для обеспечения оперативного вмешательства оператора.

А.6 Рапорты (отчеты)

Предусмотреть следующие отчетные документы, выводимые на печать и, при необходимости, на экран дисплея:

- Суточный режимный лист – автоматически выводится на печать один раз в сутки в указанное время, содержит информацию по режимным переменным.
- Отчет о нарушении режима – конфигурируется средствами системы, вызывается на печать по требованию персонала, хранится в системе не менее трех суток.
- Отчет по хозрасчетным параметрам – выводится на печать один раз в сутки средствами системы по списку.
- Отчет о наработке оборудования за месяц, за заданный период, вызывается на печать по требованию персонала;
- Отчет о переключениях механизмов за сутки, за месяц, за заданный период;

– Рапорт о фиксировании отклонения значений уставок сигнализации и блокировок от регламентных (проектных).

Формы вышеназванных документов предоставляет пользователь системы управления в соответствии с принятыми у Заказчика.

Система должна обеспечивать возможность печати указанных документов в файл формата PDF.

Приложение Б
Перечень документов, необходимых для конфигурирования системы управления

- Форма режимного листа (предоставляется Заказчиком);
- Форма отчета о нарушении режима (предоставляется Заказчиком);
- Форма отчета по хозрасчетным параметрам (предоставляется Заказчиком);
- Форма отчета о наработке оборудования за месяц, за заданный период (предоставляется Заказчиком);
- Форма отчета о переключениях механизмов за сутки, за месяц, за заданный период (предоставляется Заказчиком);
- Форма рапорта о фиксировании отклонения значений уставок сигнализации и блокировок от регламентных (предоставляется Заказчиком);
- Таблицы входных/выходных сигналов (разрабатываются Проектировщиком объекта);
- Логические схемы блокировок и управления работой оборудования (разрабатываются Проектировщиком объекта);
- Схемы сложного регулирования (при необходимости разрабатываются Проектировщиком объекта).
- Технологические схемы (разрабатываются Проектировщиком объекта).
- Дополнительная проектная документация (перечень составляется до заключения договора поставки).

Приложение В
Требования по поставке оборудования и услуг

Поставщик должен предложить систему, созданную на базе серийно выпускаемых современных технических средств и последних версий базового ПО.

Условия на поставку запчастей и обновления ПО в послегарантийный период в течение 20 лет после поставки оборудования.

Поставка прикладного ПО должна включать в себя установочные дистрибутивы, лицензионные ключи/пароли, открытый код разработанного прикладного ПО.

Укрупненный перечень оборудования для создания АСУТП представлен в таблице:

Укрупненный перечень оборудования для создания АСУТП

№ П/П	НАИМЕНОВАНИЕ И ТЕХНИЧЕСКАЯ ХАРАКТЕРИСТИКА	КОЛИЧЕСТВО, ШТ.
1	2	3
1.	Контроллерные шкафы (в сборе)	Уточняется Поставщиком АСУТП
2.	Кроссовые шкафы (в сборе)	Уточняется Поставщиком АСУТП
3.	Терминальные шкафы (в сборе)	Уточняется Поставщиком АСУТП
4.	Система бесперебойного питания (ИБП, шкафы АКБ, шкаф ввода/байпаса)	Комплект Уточняется Поставщиком АСУТП
5.	Шкафы распределения питания (в сборе) для питания оборудования	Уточняется Поставщиком АСУТП (проектируется с учетом размещения сущ. оборудования АСУТП)
6.	Сетевые коммуникационные шкафы (в сборе)	Уточняется Поставщиком АСУТП
7.	АРМ оператора	9 комплектов
8.	Локальные АРМ ОТ	8
9.	ИС	Уточняется Поставщиком АСУТП
10.	ИС резервного копирования	Уточняется Поставщиком АСУТП
11.	Тренажерный комплекс	комплект
12.	OPC сервер	1
13.	Сервер точного времени с внешней антенной для работы с глобальной навигационной системой ГЛОНАСС/GPS	1 комплект
14.	Лазерный принтер черно-белый формата А4	1
15.	Цветной принтер формата А4	1
16.	Кабели связи, питания, заземления и др. для внутрисистемного подключения оборудования (от кросс-шкафа до верхнего уровня; от ШРП до потребителей АСУТП)	Комплект
17.	Оборудование и принадлежности для внутрисистемного монтажа	Уточняется Поставщиком АСУТП
18.	Специализированное программное обеспечение с набором всех необходимых лицензий и сертификатов (с учетом резерва по сигналам ввода-вывода), включая OPC лицензии для подключения не менее 2 клиентов	Комплект
19.	Оборудование и ПО в соответствии с требованиями по обеспечению ИБ АСУТП	Комплект
20.	Программные и аппаратные средства для архивирования и восстановления данных последней актуальной версии для ОС Системы USB внешний жесткий диск на 2 Tb – 2 шт.	Комплект

21.	Необходимые программирующие, задающие и имитирующие устройства для всего поставляемого оборудования	Комплект
22.	Коммуникатор, поддерживающий устройства HART, обеспечивая пользователя возможностью осуществления настройки, обслуживания или поиска неисправностей в устройствах	1
23.	Калибратор электрических сигналов, имеющий сертификат об утверждении типа средств измерения, действующее свидетельство о первичной поверке	1
24.	Мультиметр с искробезопасным, герметичным корпусом классом не ниже IP65, с допуском к работе в опасных зонах (ATEX) класса 1, 2, 21 или 22.	1
25.	Запасные изделия и принадлежности (10 % от каждого применяемого компонента, но не менее 1 шт.), включая 1 монитор для АРМ. Под компонентами подразумевается активное оборудование, такое как: процессорный модуль, модуль связи, модуль интерфейсный, источник питания, модуль ввода-вывода, устройства АВР, коммутатор, барьер искрозащиты, реле, преобразователь интерфейса и т.п. Под компонентами не подразумеваются монтажные изделия, компоненты шкафного, кроссового оборудования, кабельная продукция, изделия и материалы.	Комплект
26.	Сервер точного времени	1 комплект
27.	Обучение оперативного технологического персонала на площадке Заказчика (один трехдневный курс для каждой из 5 бригад операторов-технологов); Обучение инженерного обслуживающего персонала Заказчика в учебном центре производителя системы (2 курса, не менее 2 человек на курс, продолжительность каждого курса не менее 5 дней); – Обучение инженерного обслуживающего персонала КИП Заказчика в учебном центре производителя системы (1 курс, не менее 2 человек на курс, продолжительность каждого курса не менее 5 дней);	1 комплект

Примечания:

1. В комплект поставки АСУТП должны входить: комплект внешних диагностических устройств, комплект специального инструмента и монтажных приспособлений для выполнения всех операций по монтажу, наладке эксплуатации и ремонту оборудования.

Приложение Г
Предварительная сводная таблица входных-выходных сигналов АСУТП

НАИМЕНОВАНИЕ БЛОКА		AI 4-20 mA, HART	AO, 4-20 mA, HART	DI (с.к. 24V DC)	DO (с.к. 220V AC)	Питание оборудования КиА 24V DC	Питание оборудования КиА 220V AC	RS-485 (Profibus не резер-ный), порты	Ethernet (Modbus TCP не резер-ный), порты	ИТОГО
1		2	3	4	5	6	7	8	9	10
ГТУ-1…ГТУ-6		1632	96	1728	576			6	6	
Резерв	20%	327	20	346	115			1	1	
Диверторы		96	12	576	576			6		
Резерв	20%	20	2	115	115			1		
Система воздушного охлаждения масла АВОМ 1…6		96	17	576				6		
Резерв	20%	20	3	115				1		
Противообледенительная система ПОС 1…6		96	24	144	48			6		
Резерв	20%	20	5	29	10					
Здание электрооборудования ЗЭО 1…6		96		384				6		
Резерв	20%	19		77						
Котел-утилизатор 1…6		1088		3328	864					
Резерв	20%	218		666	173					
Пункт подготовки газа (ППГ)		48	8	96	64					
Резерв	20%	10	2	20	13					
Компрессорная станция приборного воздуха (КСПВ)		26	8	30	18					
Резерв	20%	5	2	6	4					
Теплоцентр		104	8	128	55			1		
Резерв	20%	21	2	26	11			1		
Общестанционная система (включая РОУ, ПК-1, ПК-2, ПТ, РУСН, КРУЭ 110 кВ)		1000	44	5232	1456			4		
Резерв	20%	200	9	1047	291			1		
Итого, с резервом		6448	262	18662	5426			40	7	

AI, AO - аналоговый вход, аналоговый выход

DI, DO - дискретный вход, дискретный выход

Приложение Д
Структурная схема комплекса технических средств (КТС) АСУТП

2-ой уровень автоматизации

1-ый уровень автоматизации

0-ый уровень автоматизации

Пункт управления

Обзорные экраны

АРМ ОТ (9 шт.)

Система ИБП

Принтер (2 шт.)

Терминальная шина Industrial Ethernet

Сервер точного времени

Серверы

АРМ администратора

ИС

ИС резерв. копирования

Modbus TCP

К оборудованию

Система ИБП

Помещение ИБК

Системная шина Industrial Ethernet

Сете-вой шкаф

Сете-вой шкаф

Сете-вой шкаф

Сете-вой шкаф

МЭК 61850

К оборудованию

ГУ-1 ГУ-2 ГУ-3

ГУ-4 ГУ-5 ГУ-6

ПК-1, ПК-2

ОК об

ПТ

ППГ

КСПВ

Оборудование ЭЧСР ПТ. Приборы и исполнительные механизмы

Общестанционные приборы и исполнительные механизмы

ОС об.

ТЦ

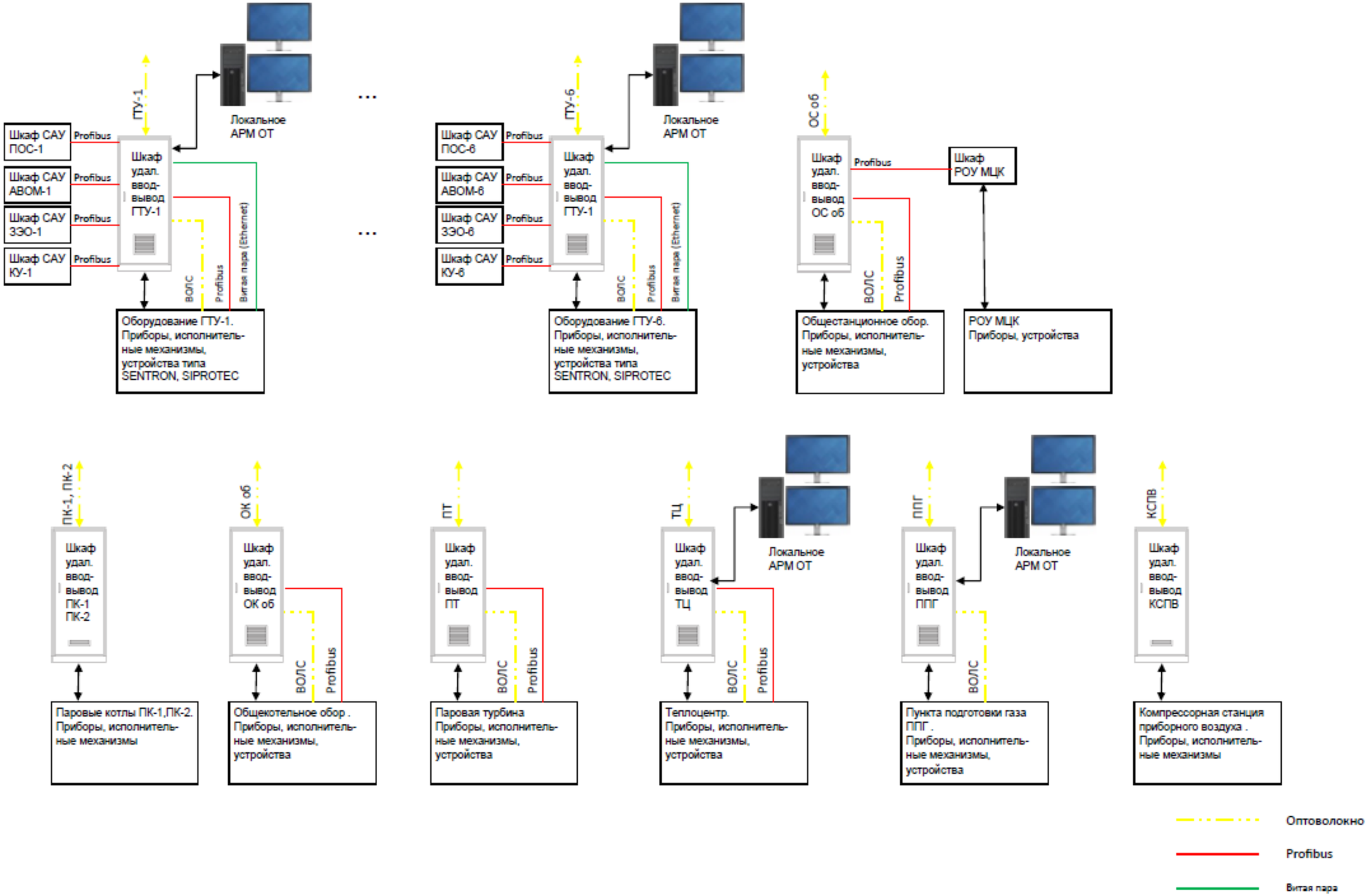
Взам. инв. №

Подпись и дата

Инв. № подл.

Изм.	Колуч	Лист	№докум	Подпись	Дата	79566035.001-ПП-700.271.005-АСУ.ТТ	Лист 60

Продолжение структурной схемы комплекса технических средств (КТС) АСУТП



Взам. инв. №

Подпись и дата

Инв. № подл.

Изм.	Колуч	Лист	№докум	Подпись	Дата	79566035.001-ПП-700.271.005-АСУ.ТТ	Лист 61

Приложение Е
Перечень документов технорабочего проекта и эксплуатационных документов, которые должны быть переданы Поставщиком Заказчику при внедрении АСУТП

Наименование документа	Обозначение по ГОСТ 34.201-2020	Примечание
Техническое задание на АСУТП		В соответствии с ГОСТ 34.602-2020
Общесистемная документация:		
Пояснительная записка к техническому проекту;	(П2)	
Общее описание системы;	(ПД)	
Описание автоматизируемых функций	(П3)	
Ведомость технорабочего проекта	(ТРП)	
Ведомость эксплуатационных документов;	(ЭД)	
Программа и методика испытаний;	(ПМ)	
Формуляр;	(ФО)	
Паспорт;	(ПС)	
Проектная оценка надежности.	(Б1)	
Локальный сметный расчет	(Б2)	
Документация технического обеспечения:		
Описание комплекса технических средств	П9	
Схема структурная комплекса технических средств	С1	
Схема соединений внешних проводок	С4	
Схема (таблица) подключения внешних проводок	С5	
Таблица соединений и подключений	С6	
Спецификация оборудования (в части поставляемого оборудования)	В4	
Инструкция по эксплуатации	ИЭ	Содержание документа должно быть выполнено, в том числе, с учетом ГОСТ 2.601-2013
Схема подключения сетей обмена информацией	СБ1	
Чертеж установки технических средств	СА	
Схемы электропитания и заземления АСУТП	СБ2	
Схемы принципиальные шкафов	СБ3	
План расположения оборудования и проводок	С7	
Типовые схемы подключения полевого оборудования (измерительных	СБ1	

преобразователей)		
Таблица распределения сигналов по модулям		
Логические схемы блокировок и управления (с адресацией).		
Документация информационного обеспечения:		
Перечень входных сигналов АСУТП;	В1	
Перечень выходных сигналов АСУТП (РСУ, ПАЗ);	В2.1	
Чертежи форм видеокадров и документов;	С9	
Перечень выходных документов (рапортов и отчетов);	В2.2	
Описание информационного обеспечения Системы	П5	
Инструкция по формированию и ведению базы данных (набора данных)	И4	
Описание системы классификации и кодирования	П7	
Документация программного обеспечения:		
Спецификация программного обеспечения;	В4.1	
Описание программного обеспечения АСУТП;	ПА	
Блок-схемы алгоритмов РСУ	С11	
Блок-схемы алгоритмов СПАЗ	С12	
Документация математического обеспечения:		
Описание алгоритмов АСУТП (РСУ, СПАЗ).	ПБ	
Документация организационного обеспечения:		
Описание организационной структуры	ПВ	
Руководство системного инженера	И3.1	
Руководство пользователя АРМ оператора	И3.2	
Документация по обеспечению ИБ АСУТП		
Ведомость монтажных работ		
Технические условия на размещение и подключение оборудования АСУТП		

Работы и перечень отчетной документации, связанные с испытанием системы должны соответствовать ГОСТ Р 59792-2021 ИТ «Виды испытаний автоматизированных систем».

Перечень требуемой отчетной документации представлен в Приложении Ж данных Технических требований.

Содержание документов должно удовлетворять требованиям НТД.

Разработчик (Поставщик) предоставляет Заказчику положительное заключение экспертизы промышленной безопасности

Приложение Ж
Перечень отчетной документации, оформляющейся в процессе приемки и монтажа оборудования АСУТП, проведения всех видов испытаний и по их завершению

№	Наименование документа	Заказчик	Поставщик
1	Протокол №1 проверки комплектности поставленного оборудования АСУТП и сопроводительной документации	+	+
2	Акт приема передачи оборудования АСУТП	+	+
3	Акт готовности объекта к выполнению монтажных работ	+	+
4	Акт приема-передачи оборудования АСУТП в монтаж	+	+
5	Акт приемки оборудования АСУТП по завершению монтажных работ		+
6	Акт о проверке сопротивления контуров заземления		+
7	Акт о проверке выполненных подключений системных кабелей		+
8	Акт о проверке выполненных подключений сигнальных кабелей		+
9	Акт о проверке выполненных подключений оптического кабеля, с измерением оптических параметров		+
10	Акт о проверке выполненных подключений кабелей электропитания, с проверкой сопротивления изоляции от ЩРП до вводных клемм комплекса технических средств АСУТП		+
11	Акт приемки оборудования АСУТП после индивидуальных испытаний	+	+
12	Протокол №2 по выполнению ПНР по пуску систем бесперебойного питания		+
13	Протокол №3 проверки функционирования КТС АСУТП		+
14	Протокол №4 проверки комплектности документации ТРП	+	+
15	Протокол №5 принятия прикладного ПО	+	+
16	Протокол №6 проверки отказоустойчивости и функций самодиагностики АСУТП		+
17	Акт №1 завершения автономных испытаний АСУТП	+	+
18	Программа комплексных испытаний		+
19	Протокол №7 проверки измерительных каналов КТС АСУТП		+
20	Акт №2 завершения комплексных испытаний АСУТП	+	+
21	Протокол №8 обучения оперативного (технологического) персонала		+
22	Акт №3 о приемки АСУТП в опытную эксплуатацию	+	+
23	Программа опытной эксплуатации		+
24	Акт №4 о завершении опытной эксплуатации АСУТП	+	+
25	Протокол №9 проведения приемочных испытаний, предусмотренных программой испытании		+
26	Протокол №10 о соответствии системы требованиям ТЗ на АСУТП	+	+
27	Акт №5 приемки АСУТП в промышленную эксплуатацию, в объеме, предусмотренном проектом.	+	+

Приложение 3
Перечень инжиниринговых работ по АСУТП, выполняемых поставщиком

Конфигурирование контроллеров АСУТП:

1. Конфигурирование контроллеров системы управления:

- Конфигурирование сетевых адресов контроллеров системы управления;
- Конфигурирование общих данных контроллеров системы управления;
- Конфигурирование модулей входов/выходов контроллеров системы управления;
- Конфигурирование базы данных дискретных входов/выходов контроллеров системы управления;
- Конфигурирование базы данных аналоговых входов/выходов контроллеров системы управления;
- Конфигурирование функциональных блоков контроллеров системы управления;
- Конфигурирование интерфейсного обмена с подсистемами.
- Разработка расчета загрузки контроллеров системы управления.

2. Конфигурирование алгоритмов управления оборудованием:

- Разработка стратегий управления оборудованием;
- Конфигурирование схем управления и индикации согласно перечню сигналов ввода/вывода и функциональных/логических схем:
  - аналоговых измерительных;
  - аналоговых регулирующих;
  - дискретных;
  - информационных;
  - логических для клапанов;
  - логических для электроприводов.
- Конфигурирование функциональных блоков управления оборудованием контроллеров;
- Конфигурирование функциональных блоков каскадного регулирования и т.п. контроллеров;
- Формирование списка логических переменных, соответствующих сигнализационным сообщениям;
- Конфигурирование сигнализационных сообщений контроллеров;
- Конфигурирование сообщений оператору;
- Конфигурирование вспомогательных (промежуточных) логических переменных (переключателей);
- Конфигурирование нестандартных программ управления контроллеров;

- Конфигурирование нестандартных расчетных программ контроллеров;
- Конфигурирование переменных интерфейсного обмена с подсистемами;
- Конфигурирование интерфейсного обмена с локальной заводской сетью;

3. Конфигурирование контроллеров системы безопасности:

- Конфигурирование сетевых адресов контроллеров системы безопасности;
- Конфигурирование общих данных контроллеров системы безопасности;
- Конфигурирование модулей входов/выходов контроллеров системы безопасности;
- Конфигурирование базы данных дискретных входов/выходов контроллеров системы безопасности;
- Конфигурирование базы данных аналоговых входов/выходов контроллера системы безопасности;
- Конфигурирование функциональных блоков контроллера системы безопасности;
- Конфигурирование интерфейсного обмена с системой управления;
- Разработка расчета загрузки контроллеров системы безопасности.

4. Конфигурирование логических схем блокировок и защит технологического оборудования:

- Разработка стратегий (схемы) блокировок системы безопасности;
- Конфигурирование функциональных блоков схем блокировок и защит оборудования контроллера;
- Формирование списка логических переменных, соответствующих аварийным (блокировочным) сообщениям;
- Конфигурирование аварийных сообщений системы безопасности;
- Конфигурирование сообщений оператору по системе безопасности;
- Конфигурирование вспомогательных (промежуточных) логических переменных (переключателей);
- Конфигурирование ключей пусковых деблокировок;
- Конфигурирование деблокирующих ключей обслуживания полевого оборудования;
- Конфигурирование переменных интерфейсного обмена с системой управления.

5. Конфигурирование станций оператора:

- Разработка графических дисплеев (мнемосхем) управления технологическим процессом в соответствии с монтажно-технологическими схемами объекта автоматизации (Создание видеокадров управления технологическим оборудованием);
- Разработка и конфигурирование видеокадров системы блокировок;

- Придание динамических свойств графическим объектам согласно принятым обозначениям;
- Конфигурирование групп управления;
- Конфигурирование групп трендов;
- Конфигурирование функциональных клавиш операторских клавиатур для каждого рабочего места (при их наличии);
- Конфигурирование списка пользователей и уровней доступа пользователей к системе;
- Конфигурирование обзорного экрана;
- Конфигурирование сменных рапортов и отчетов;
- Конфигурирование архивов и переменных архивирования (исторических групп);
- Конфигурирование станции инженера КИП (конфигурирование/создание базы КИП).

6.Тестирование разработанного программного обеспечения:

- Проверка и отладка разработанного программного обеспечения. Устранение замечаний.

7. Проверка передачи данных от АСУТП через OPC.

Приложение И
Перечень пусконаладочных работ и испытаний по АСУТП, выполняемых поставщиком

Выполнение пусконаладочных работ и испытаний на площадке заказчика

1. Проведение индивидуальной наладки КТС АСУТП:

- Подача электропитания на компоненты АСУТП;
- «Холодный» пуск контроллеров подсистем АСУТП;
- Визуальная проверка индикаторов состояния контроллеров подсистем;
- Установка и загрузка системного программного обеспечения на станциях оператора и инженерной;
- Установка и загрузка прикладного ПО с инженерных станций;
- Загрузка системного и прикладного программного обеспечения в контроллеры подсистем;
- Проверка состояния контроллеров подсистем, систем ввода/вывода по системным экранам и системным сигнализационным сообщениям;
- Устранение неисправностей, возникших на этапе индивидуальных испытаний АСУТП.

2. Проведение автономных испытаний КТС АСУТП:

- Проверка комплектности поставки документации техно-рабочего проекта согласно спецификации договора и ТЗ;
- Проведение предварительных испытаний на соответствие системы Техническому заданию в соответствии с программой предварительных испытаний (программу испытаний разрабатывает поставщик системы и утверждает заказчик).
- Тестирование и наладка аппаратных компонентов системы: центральной части (контроллеров, модулей в/в), сетевых соединений, оборудования верхнего уровня, тестирование функций резервирования оборудования;
- Проверка работоспособности периферийных устройств АСУТП, наладка, устранение неисправностей;
- Проверка работоспособности интерфейсов связи с подсистемами и интерфейсных конверторов, шинных преобразователей, наладка, устранение неисправностей;
- Автономная проверка и отладка прикладного программного обеспечения (базы данных, алгоритмов блокировок, логики, дисплеев визуализации и т.д.) подсистем АСУТП совместно с представителями Заказчика. Устранение неисправностей. Объем базы данных определяется количеством каналов ввода/вывода в соответствии с исходными данными:

1. Графические мнемокадры-мнемосхемы;
2. Тренды – для всех аналоговых точек (вход/выход);
3. Операционные среды персонала с защитой доступа и функциональные клавиатуры;
4. Архив и отчеты;
5. Хозрасчетные параметры;
6. Анализ результатов испытаний и устранение недостатков, выявленных в процессе испытаний, а также внесение изменений в проектную документацию по необходимости.

- Проверка подключений полевого оборудования к подсистемам КТС АСУТП совместно с представителем Заказчика (пуско-наладочной организацией по полевому оборудованию);
- Проведение подготовительных работ и предварительных испытаний станции конфигурирования и диагностики оборудования КИПиА.

3. Поверка КТС АСУТП:

- Метрологическая поверка измерительных каналов подсистем КТС АСУТП;

4. Проведение комплексных испытаний АСУТП:

- проверка всех подсистем АСУТП в комплексе вместе с полевым оборудованием. Работы выполняются с проверкой алгоритмов управления воздействия на исполнительные механизмы с проверкой их отработки, имитации входных сигналов, взаимодействия периферийных устройств. Определение соответствия порядка отработки исполнительных устройств и элементов систем сигнализации, защиты и управления алгоритмам рабочей документации с выявлением причин отказа или «ложного» срабатывания, установка необходимых значений срабатывания позиционных устройств;
- Проверка выполняется согласно документов ТРП и утвержденной программе проведения испытаний на площадке заказчика;
- настройка логических и временных взаимосвязей систем сигнализации;
- настройка логических и временных взаимосвязей систем защиты;
- настройка логических и временных взаимосвязей систем блокировки;
- настройка логических и временных взаимосвязей контуров управления;
- первичная настройка логических и временных взаимосвязей контуров управления (первичная настройка ПИД-регуляторов);
- сдача Системы в опытную эксплуатацию: уточнение статических и динамических характеристик объекта, корректировка значений, параметров настройки систем с

учётом их взаимного влияния в процессе работы, корректировка настроек логических и временных взаимосвязей контуров управления (настройка ПИД-регуляторов в соответствии с требованиями технологического процесса), подготовка и передача Заказчику данных по настройке контуров управления (ПИД-регуляторов), подготовка рекомендаций Заказчику.

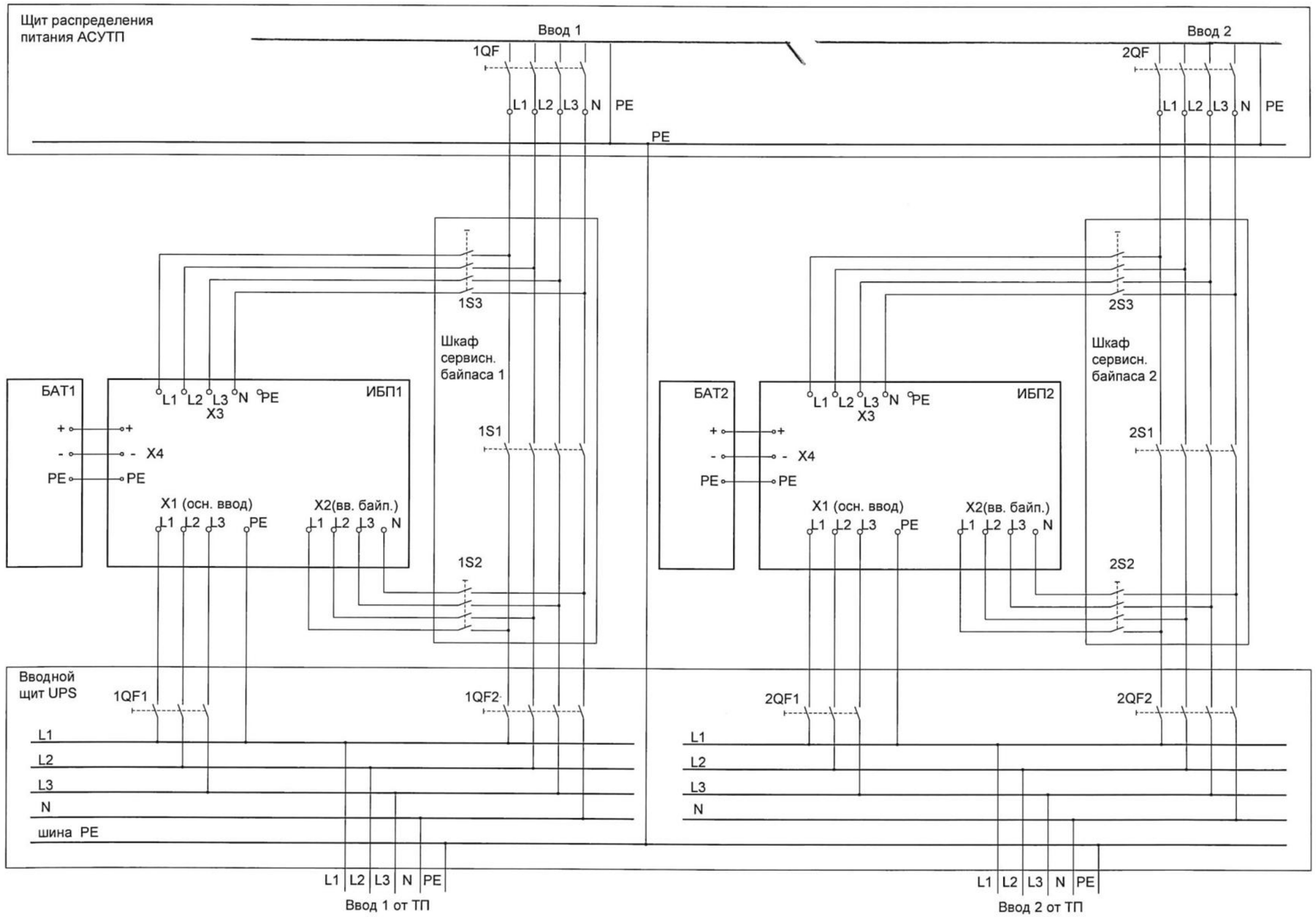
5. Опытная эксплуатация в части автоматизации до момента вывода установки на устойчивый штатный режим и сдачи в промышленную эксплуатацию:

- Срок участия Поставщика/Разработчика АСУТП в опытной эксплуатации не менее 1 месяца;
- уточнение статических и динамических характеристик объекта, корректировка значений параметров настройки систем с учётом их взаимного влияния в процессе работы;
- корректировка настроек логических и временных взаимосвязей контуров управления (настройка ПИД-регуляторов в соответствии с требованиями технологического процесса), подготовка и передача Заказчику данных по настройке контуров управления (ПИД-регуляторов);
- подготовка рекомендаций Заказчику.

6. Проведение приёмочных испытаний АСУТП:

- проверка рабочего журнала опытной эксплуатации;
- устранение замечаний и рекомендаций;
- ревизия проектной документации и внесение изменений (при необходимости);
- сдача Системы в промышленную эксплуатацию.

Приложение К
Пример структурной схемы электропитания АСУТП

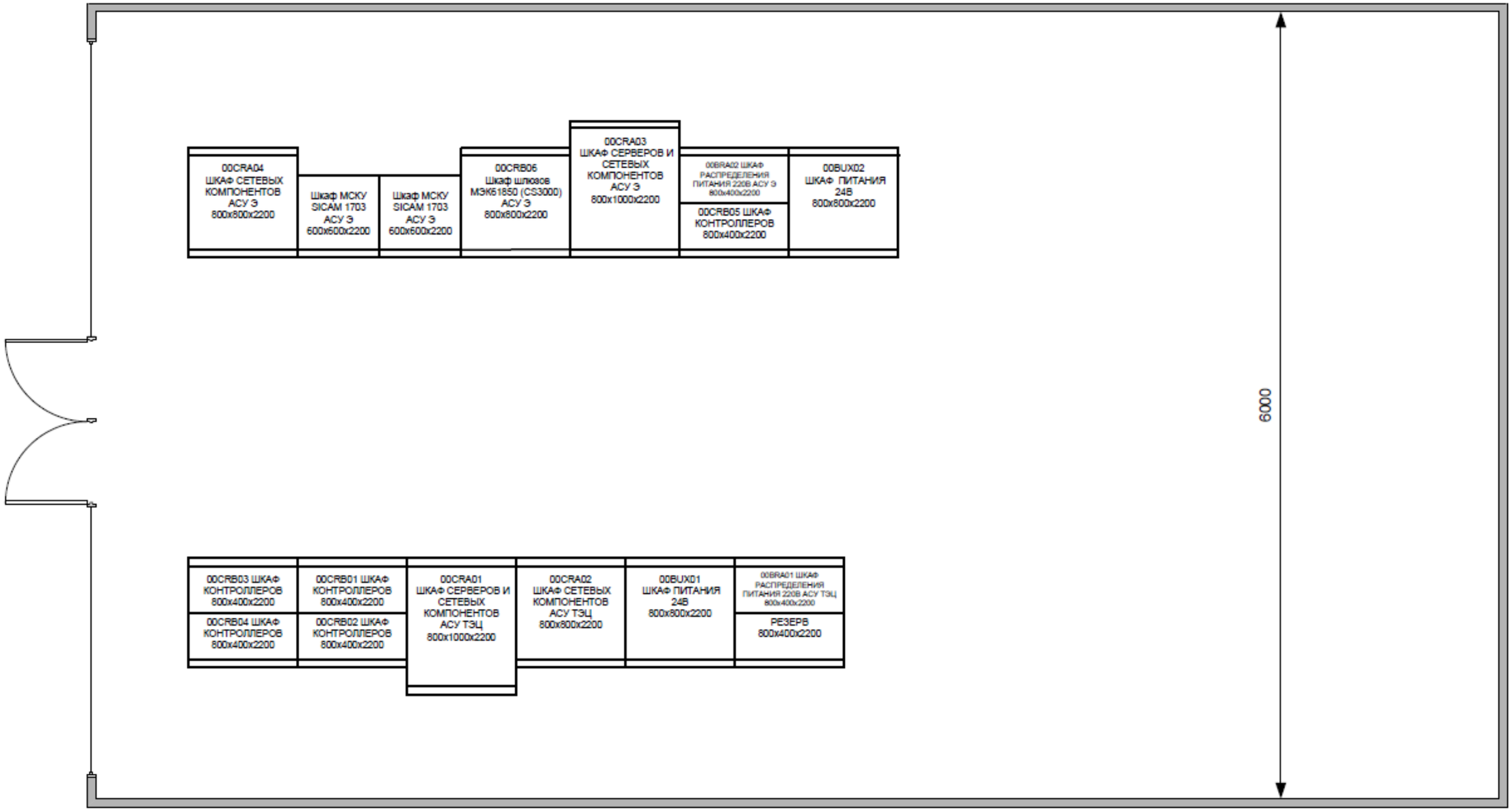


Взам. инв. №	
Подпись и дата	
Инв. № подл.	

Изм.	Колуч	Лист	№докум	Подпись	Дата	79566035.001-ПП-700.271.005-АСУ.ТТ	Лист 72

Приложение Л
Планы размещения оборудования АСУТП

Предварительный план размещения оборудования АСУТП в помещении ИБК (на основании существующего оборудования)



Помещение ИБК (к. 416) на отметке +12.300

Взам. инв. №
Подпись и дата
Инв. № подл.

Изм.	Колуч	Лист	№докум	Подпись	Дата	79566035.001-ПП-700.271.005-АСУ.ТТ	Лист 73

Приложение М
Требования по обеспечению информационной безопасности АСУТП

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

Принимаемые организационные и технические меры по обеспечению информационной безопасности должны:

- обеспечивать доступность обрабатываемой в автоматизированной системе управления технологическим процессом информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации);
- соотноситься с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности автоматизированной системе управления технологическим процессом и управляемого (контролируемого) объекта и (или) процесса;
- не оказывать отрицательного влияния на штатный режим функционирования автоматизированной системе управления технологическим процессом, с учетом требований Федерального закона от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов».

1. ПОЛНОЕ НАИМЕНОВАНИЕ СИСТЕМЫ И ЕЁ УСЛОВНОЕ ОБОЗНАЧЕНИЕ

Полное наименование системы: «Автоматизированная система управления технологическими процессами объектом «Газотурбинная установка – тепловая электростанция» на «РН-Туапсинский НПЗ».

Условное обозначение системы: АСУТП ГТУ-ТЭС.

Далее по тексту: Система.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АУТЕНТИФИКАЦИЯ	Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в Системе). [Термины и определения корпоративного глоссария]
ДЕМИЛИТАРИЗОВАННАЯ ЗОНА	Пограничный сегмент сети Системы с внешними по отношению к ней сетями (также известный как защищенная подсеть), выполняющий функции «нейтральной зоны» между указанными сетями.

	[Термины и определения настоящего документа]
ДОСТУПНОСТЬ ИНФОРМАЦИИ	Состояние информации, характеризуемое способностью автоматизированной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия. [Термины и определения корпоративного глоссария]
ЗНАЧИМЫЙ ОБЪЕКТ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	Объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры. [Федеральный закон от 26.07.2017 № 187-ФЗ]
ИДЕНТИФИКАТОР	Уникальный признак субъекта или объекта доступа. [Термины и определения настоящего документа]
ИДЕНТИФИКАЦИЯ	Присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. [Термины и определения корпоративного глоссария]
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМЫ	Составная часть безопасности, отражающая влияние свойств (целостности, доступности, конфиденциальности и др.) информации, обрабатываемой и производимой Системы, на безопасность и надежность ее функционирования. [Термины и определения настоящего документа]
ИНЦИДЕНТ	Появление одного или нескольких нежелательных, или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций, нарушения штатного функционирования Системы и создания угрозы информационной безопасности. [Термины и определения настоящего документа]
КАТЕГОРИЯ ЗНАЧИМОСТИ	Категория значимости объекта критической информационной инфраструктуры в соответствии с требованиями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». [Федеральный закон от 26.07.2017 № 187-ФЗ]
КЛАСС ЗАЩИЩЕННОСТИ	Класс защищенности АСУТП / ИС / СТМ в соответствии с требованиями приказа ФСТЭК РФ от 14.03.2014 № 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». [Федеральный закон от 26.07.2017 № 187-ФЗ]
КОМПЕНСИРУЮЩАЯ МЕРА	Мера по защите информации в Системе, дополнительно предпринимаемая в связи с практической невозможностью безусловно применить набор мер, формально определенных установленным классом защищенности Системы. [Термины и определения настоящего документа]
КОНТРОЛИРУЕМАЯ ЗОНА	Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств. [Термины и определения настоящего документа]
КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ	Свойство информации, отражающее установленное обладателем и обязательное для выполнения требование к лицу, получившему доступ к информации, не передавать такую информацию кому-либо. [Термины и определения настоящего документа]
КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	Объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. [Федеральный закон от 26.07.2017 № 187-ФЗ]
НАРУШИТЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах. [Термины и определения корпоративного глоссария]
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	Реализация комплекса организационных и технических мер по защите информации и систем автоматизации от широкого спектра угроз (в отношении целостности, доступности и конфиденциальности обрабатываемой и хранящейся информации) с целью обеспечения функционирования Системы. [Термины и определения настоящего документа]
ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. [Федеральный закон от 26.07.2017 № 187-ФЗ]
ПЕРИМЕТР СИСТЕМЫ	Физическая и (или) логическая граница Системы (сегмента Системы), в пределах которой Владельцем Системы обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации. [Термины и определения настоящего документа]

ПОЛЬЗОВАТЕЛЬ СИСТЕМЫ	Любой работник, который в процессе своей трудовой деятельности обращается к средствам вычислительной техники, применяемым в Системе, с запросом на выполнение работ. [Термины и определения настоящего документа]
ПОДРЯДНАЯ ОРГАНИЗАЦИЯ	физическое или юридическое лицо, которое выполняет работы по договору подряда, заключаемому с заказчиком в соответствии с Гражданским кодексом Российской Федерации. [Термины и определения корпоративного глоссария]
РОЛЬ	Совокупность полномочий, установленных в локальном нормативном, распорядительном документе, трудовом или ином договоре, предоставляемых исполнителю/ участнику бизнес-процесса, необходимых для выполнения бизнес-процесса в зоне его ответственности. [Термины и определения настоящего документа]
СЕГМЕНТ СИСТЕМЫ	Совокупность нескольких компонентов Системы, использующих общую (в том числе разделяемую) среду передачи и объединенных для единства решения функциональных задач. [Термины и определения настоящего документа]
СОБЫТИЕ БЕЗОПАСНОСТИ (ИНФОРМАЦИОННОЙ)	Идентифицированное возникновение состояния Системы (сегмента, компонента Системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации. [Термины и определения настоящего документа]
СУБЪЕКТ ДОСТУПА	Пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа. [Федеральный закон от 26.07.2017 № 187-ФЗ]
СУБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают

	взаимодействие указанных систем или сетей. [Федеральный закон от 26.07.2017 № 187-ФЗ]
УДАЛЕННЫЙ ДОСТУП	Процесс получения доступа (через внешнюю сеть) к объектам доступа Системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с Системой, к которой он получает доступ. [Термины и определения настоящего документа]
УПРАВЛЕНИЕ ДОСТУПОМ	Ограничение и контроль доступа субъектов доступа к объектам доступа в соответствии с установленными правилами разграничения доступа. [Термины и определения настоящего документа]
УЯЗВИМОСТЬ	Свойство информационной системы, обуславливающее возможность реализации угроз безопасности, обрабатываемой в ней информации. [Термины и определения настоящего документа]
ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ	Состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право. [Термины и определения корпоративного глоссария]

3. СОКРАЩЕНИЯ

АВЗ	Антивирусная защита.
АРМ	Автоматизированное рабочее место.
АСО	Активное сетевое оборудование.
БД	База данных.
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.
ДМЗ	Демилитаризованная зона.
ИБ	Информационная безопасность
ИБП	Источник бесперебойного питания.
КИИ	Критическая информационная инфраструктура.
Компания	ПАО «НК «Роснефть».
КИПиА	Контрольно-измерительные приборы и автоматика.
КЗ	Категория значимости
ЛНД	Локальные нормативные документы.
МЭ	Межсетевой экран.
ОГ	Общество группы.
ОПР	Основные проектные решения.
ОС	Операционная система.
ППО	Прикладное программное обеспечение.
ПНР	Пуско-наладочные работы.
ПО	Программное обеспечение.
РФ	Российская Федерация.
СМСТСПА	Система мониторинга сетевого трафика систем промышленной автоматизации.
СЗИ	Средство(а) защиты информации.
ТЗ	Техническое задание.
УЗ	Учетная запись.
BIOS	Базовая система ввода-вывода.

4. ОБЩИЕ ПОЛОЖЕНИЯ

Выбор мер защиты информации для их реализации в Системе в рамках её системы защиты включает:

- определение базового набора мер защиты информации для установленного класса защищённости / категории значимости Системы;
- адаптацию базового набора мер защиты информации применительно к каждому уровню Системы, иным структурно-функциональным характеристикам и особенностям функционирования Системы (в том числе предусматривающую исключение из базового набора мер защиты информации, мер, непосредственно связанных с технологиями, не используемыми в Системе или её уровнях, или структурно-функциональными характеристиками, не свойственными Системе);
- уточнение адаптированного базового набора мер защиты информации с учётом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз ИБ на каждом из уровней Системы;
- дополнение уточнённого адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований к защите информации, установленными нормативными правовыми актами РФ в области защиты информации, ЛНД Компании в области ИБ.

Выбор базового набора мер защиты основан на присвоенном классе защищенности Системы по требованиям защиты информации либо присвоенной категории значимости объекта КИИ.

Выбранные меры защиты информации рассматриваются для каждого уровня автоматизации Системы отдельно и подлежат реализации с учетом особенностей функционирования каждого из уровней.

Организационно-распорядительная документация по мерам защиты информации объекта КИИ должна разрабатываться в соответствии с Положением Компании от 19.06.2020 № ВР3-11-01_R-0220 "Обеспечение безопасности объектов КИИ" и Перечнем состава документов по безопасности значимых объектов КИИ, утвержденным Компанией.

В проектной документации должно быть приведено обоснование достаточности выбранных мер защиты информации для нейтрализации угроз ИБ и обеспечения необходимого уровня защищенности Системы.

Для обеспечения ИБ Системы при выборе СЗИ необходимо руководствоваться рекомендациями Компании.

Принимаемые технические меры защиты информации:

- должны обеспечивать доступность обрабатываемой в Системе информации (исключение неправомерного блокирования информации), 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 Системы и управляемого (контролируемого) объекта и (или) процесса;

- не должны оказывать отрицательного влияния на штатный режим функционирования Системы с учетом требований Федерального закона от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов».

5. КЛАСС ЗАЩИЩЁННОСТИ / КАТЕГОРИЯ ЗНАЧИМОСТИ СИСТЕМЫ

В соответствии с требованиями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» Системе предварительно присвоена категория значимости: КЗ-3.

6. КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ К ПОДРЯДНОЙ ОРГАНИЗАЦИИ

Подрядная организация должна обладать практическим опытом выполнения работ по обеспечению ИБ не менее 3 лет и иметь лицензию ФСТЭК РФ на деятельность по технической защите конфиденциальной информации на соответствующие виды работ и услуг в рамках требований постановления Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

Для выполнения работ по проектированию и внедрению СЗИ Подрядной организацией должны быть включены в проектную команду специалисты, удовлетворяющие следующим требованиям к квалификации:

- имеющие высшее образование по направлению подготовки (специальности) в области ИБ и стаж в области проводимых работ не менее 5 лет – не менее 1 специалиста
- имеющие высшее образование по направлению подготовки (специальности) в области ИБ и стаж в области проводимых работ не менее 3 лет – не менее 1 специалиста.

Подрядная организация на дату проведения работ не должна иметь каких-либо зафиксированных невыполненных договорных обязательств по ИБ в отношении ОГ Компании.

7. ТРЕБОВАНИЯ К МЕРАМ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ

Информационная безопасность компонентов Системы должна обеспечиваться такими техническими мерами и решениями, которые полностью исключают или эффективно ограничивают возможности как самопроизвольного, так и умышленного искажения сигналов и данных в Системе, способного приводить к неблагоприятным последствиям.

Набор технических мер защиты информации[1] сформирован на основе присвоенного класса защищённости / категории значимости Системы.

В случае, если определенные меры, приведенные в данном разделе, уже реализованы, то это должно быть учтено на этапе проектирования.

7.1. ТРЕБОВАНИЯ К ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА (ИАФ)

(ИАФ.0, ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.7)

Для обеспечения идентификации и аутентификации в Системе должны выполняться меры:

- регламентация правил и процедур идентификации и аутентификации (ИАФ.0);
- идентификация и аутентификация Пользователей и инициируемых ими процессов (ИАФ.1);
- идентификация и аутентификация устройств (ИАФ.2);
- управление идентификаторами (ИАФ.3);
- управление средствами аутентификации (ИАФ.4);
- идентификация и аутентификация внешних Пользователей (ИАФ.5);
- защита аутентификационной информации при передаче (ИАФ.7).

Данные меры должны быть реализованы за счёт использования встроенных в BIOS, ОС, ППО и встроенное ПО Системы механизмов защиты информации, средств АВЗ, АСО, МЭ и иных СЗИ, разработки правил и процедур идентификации и аутентификации, регламентации предоставления доступа.

Общие требования к ИАФ:

Учётные данные, используемые в Системе и её СЗИ, должны создаваться в соответствии с требованиями ЛНД Компании в области обеспечения защиты информации. Механизмы идентификации и аутентификации ОС, ППО, АСО, АВЗ, МЭ должны обладать следующими функциональными характеристиками:

- возможность задания произвольной длины пароля, состоящего из цифро-буквенных символов верхнего и нижнего регистра, а также специальных символов, минимальной сложности пароля (длина пароля должна быть не менее 8 символов и состоять из цифр, букв и специальных символов);

[1] Обозначение и наименование мер защиты даны в соответствии с требованиями приказа ФСТЭК РФ от 14.03.2014 № 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» и требованиями приказа ФСТЭК РФ от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

- возможность ограничения срока действия пароля;
- возможность запрета повторного использования пароля;
- возможность уведомления Пользователя Системы о необходимости смены пароля;
- хранение паролей доступа в Систему в защищенном виде;
- ограничение неуспешных попыток входа в Систему (блокировка учетной записи после 5 неуспешных попыток доступа);
- при смене пароля:
  - возможность двойного подтверждения при самостоятельной смене пароля;
  - возможность автоматического сброса поля ввода после каждой проверки введенного пароля;
- парольный ввод в Систему должен осуществляться:
  - без отображения истинных символов в поле ввода;
  - с двойным подтверждением при самостоятельной смене;
  - со сбросом поля ввода после каждой проверки введенного пароля;
- хранение и передача по сети паролей доступа в Систему должно осуществляться в защищенном виде. Запрещается хранить и передавать пароли в незащищенном виде;
- пароли, создаваемые по умолчанию, в том числе к системным и служебным учетным записям, а также служебные коды доступа к контроллерам и оборудованию КИПиА должны быть изменены после инсталляции системы и/или монтажа оборудования перед запуском Системы в эксплуатацию.

7.2. ТРЕБОВАНИЯ К УПРАВЛЕНИЮ ДОСТУПОМ СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА (УПД)

(УПД.0, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.13, УПД. 14)

Для управления доступом в Системе должны выполняться меры:

- регламентация правил и процедур управления доступом (УПД.0);
- управление учетными записями Пользователей (УПД.1);
- реализация модели (политик) управления доступом (УПД.2);
- разделение полномочий (ролей) Пользователей (УПД.4);
- назначение минимально необходимых прав и привилегий (УПД.5);
- ограничение неуспешных попыток доступа в Систему (УПД.6);
- блокирование сеанса доступа Пользователя при неактивности (УПД.10);
- управление действиями Пользователей до идентификации и аутентификации (УПД.11);
- реализация защищенного удаленного доступа (УПД.13);
- контроль доступа из внешних информационных (автоматизированных) систем (УПД.14).

Данные меры должны быть реализованы за счёт использования встроенных в ОС, ППО, встроенное ПО Системы механизмов защиты информации, средств АВЗ, АСО, МЭ и иных СЗИ, разработки правил и процедур управления доступом, регламентации предоставления доступа.

Общие требования к УПД:

При реализации доступа работников к компонентам Системы необходимо обеспечить:

- возможности настройки минимально необходимых полномочий для решения производственных задач;
- возможности отключения всех дополнительных прав работников и функционала систем;
- возможности настройки права доступа на уровне модулей ППО Системы;
- возможности настройки права доступа на уровне БД Системы, при этом доступ работников к БД, используемых в Системе, должен быть ограничен. Доступ к БД должен быть разрешен только администраторам Системы и только при условии регистрации всех событий и действий работника в БД. Все действия, совершаемые работниками в БД должны регистрироваться в журналах БД либо в специальных системах контроля действий Пользователей БД;
- возможности настройки права доступа на уровне ОС серверов управления и АРМ;
- возможности настройки права доступа на уровне контроллеров и оборудования нижнего уровня Системы (уровня КИПиА);
- при предоставлении прав и привилегий по доступу к компонентам Системы:
- возможность разделять права таким образом, чтобы у одного лица не было полного контроля над всеми компонентами Системы;
- возможность разделения прав администрирования по компонентам Системы – РСУ, ПАЗ, КИПиА;
- исключение неконтролируемого совершения операций в Системе другими лицами;
- возможность управления доступом на уровне ролей. При этом минимальный набор ролей на уровне ППО Системы должен включать:
  - роль, реализующую функции администратора Системы, включающие внесение изменений в состав и конфигурацию Системы, установку и инициализацию модулей ПО, создание учетных записей работников и управление правами доступа;
  - роль, реализующую функции оператора Системы, включающие осуществление задач по контролю и управлению технологическим процессом, без возможностей внесения изменений в состав и конфигурацию компонентов Системы.
- возможность мониторинга и контроля средствами ОС, АВЗ и иных СЗИ за применением мобильных технических средств (флэш-накопители, внешние накопители на жестких дисках, ноутбуки, нетбуки, планшеты, смартфоны, цифровые камеры, звукозаписывающие устройства и иные устройства);
- все действия по созданию учетных записей (идентификаторов), присвоения и изменения прав доступа к компонентам Системы должны регистрироваться в журналах Системы;
- запуск компонентов прикладного ПО, предназначенных для работы Пользователей с Системой, должен выполняться от имени непривилегированной учетной записи.

7.3. ТРЕБОВАНИЯ К ОГРАНИЧЕНИЮ ПРОГРАММНОЙ СРЕДЫ (ОПС)

Требования не предъявляются, так как Системе присвоена категория значимости К3-3.

7.4. ТРЕБОВАНИЯ К ЗАЩИТЕ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ (ЗНИ)

(ЗНИ.0, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.7, ЗНИ.8)

Для обеспечения ЗНИ в Системе должны выполняться меры:

- регламентация правил и процедур защиты машинных носителей информации (ЗНИ.0);
- учёт машинных носителей информации (ЗНИ.1);
- управление физическим доступом к машинным носителям информации (ЗНИ.2);
- контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации (ЗНИ.5);
- контроль подключения съемных машинных носителей информации (ЗНИ.7);
- уничтожение (стирание) информации на машинных носителях информации (ЗНИ.8).

Данные меры должны быть реализованы за счёт использования встроенных в BIOS и ОС механизмов защиты информации, средств АВЗ и иных СЗИ, разработки правил и процедур защиты машинных носителей информации.

Общие требования к ЗНИ:

В BIOS АРМ операторов и инженерных станций Системы, серверов управления Системы должна быть запрещена загрузка ОС с иных носителей, кроме системного жесткого диска компьютеров и серверов.

При отсутствии производственной необходимости, все интерфейсы и устройства ввода-вывода на съемные носители, включая порты USB, IEEE 1394, порты карт памяти, устройства чтения и записи на оптические и магнитные диски должны быть отключены, а возможность чтения/записи с/на съемные носители должна быть заблокирована с использованием механизмов защиты ОС или СЗИ.

Должна быть предусмотрена возможность физического ограничения доступа к машинным носителям информации устройств (АРМ, серверы, ПЛК, КИПиА) посредством опломбирования корпусов и интерфейсов (пломбировочные материалы должны быть включены в состав поставки Системы).

Все факты использования съемных носителей информации, с указанием совершенных операций (чтения/записи с/на носитель) должны регистрироваться в соответствующих системных журналах (ОС, СЗИ) с указанием времени регистрации события, совершенной операции, имени активного Пользователя в ОС компонента Системы.

7.5. ТРЕБОВАНИЯ К АУДИТУ БЕЗОПАСНОСТИ (АУД)

(АУД.0, АУД.1, АУД.2, АУД.3, АУД.4, АУД.6, АУД.7, АУД.8, АУД.10)

Для обеспечения аудита безопасности в Системе должны выполняться меры:

- регламентация правил и процедур аудита безопасности (АУД.0);
- инвентаризация информационных ресурсов (АУД.1);
- анализ уязвимостей и их устранение (АУД.2);
- генерирование временных меток и (или) синхронизация системного времени (АУД.3);
- регистрация событий безопасности (АУД.4);
- защиту информации о событиях безопасности (АУД.6);
- мониторинг безопасности (АУД.7);
- реагирование на сбои при регистрации событий безопасности (АУД.8);
- проведение внутренних аудитов (АУД.10).

Данные меры защиты должны быть реализованы за счет использования встроенных в ОС, ППО, АСО механизмов защиты, АВЗ, МЭ и иных СЗИ, разработки правил и процедур аудита безопасности.

Общие требования к АУД:

В ОС и ППО Системы должна осуществляться регистрация:

- событий безопасности;
- вход/выход Пользователей, включая неуспешные попытки доступа, с указанием идентификатора Пользователя, даты и времени события;
- создание, удаление, изменение привилегий Пользователей;
- действия операторов, администраторов Системы, по внесению изменений в конфигурацию и настройки Системы, формирование команд и операций в Системе, операции с журналами регистрации;
- совершаемые технологические операции, транзакции в Системе и параметры операций, включая дату и время совершения операции, и иные параметры;
- системные ошибки;
- изменение параметров конфигурации ПО, состава компонентов Системы, установка/удаление программ и обновлений;
- старт/стоп событий и процессов, запуск/останов особых режимов работы ПО и оборудования Системы;
- доступ к объектам системы – файлам конфигурации, файлам данных, файлам журналов регистрации.

Средства АВЗ должны регистрировать следующие виды событий:

- факт отключения защиты;
- обнаружение вирусов и дальнейшие действия с объектом;
- изменение состояния антивирусных средств;
- установка и распространение обновлений.

Время хранения журналов событий:

- на антивирусном сервере – не менее 2 месяцев;
- журналов событий ОС, ППО – не менее 1 года (со дня фиксации последнего события).

7.6. ТРЕБОВАНИЯ К АНТИВИРУСНОЙ ЗАЩИТЕ (АВЗ)

(АВЗ.0, АВЗ.1, АВЗ.2, АВЗ.4)

Для обеспечения АВЗ в Системе должны выполняться меры:

- регламентация правил и процедур антивирусной защиты (АВЗ.0);
- реализация АВЗ (АВЗ.1);
- АВЗ электронной почты и иных сервисов (АВЗ.2);
- обновление БД признаков вредоносных компьютерных программ (вирусов) (АВЗ.4);

Данные меры должны быть реализованы за счёт использования средств АВЗ, МЭ, СОВ, разработки правил и процедур антивирусной защиты.

Общие требования к АВЗ:

- АВЗ должна быть реализована на уровне файловой системы АРМ и серверов Системы, а также МЭ (в случае его применения);
- средства АВЗ должны поставляться исходя из количественного состава технических средств Системы, на которых предполагается их применение, с лицензиями на срок эксплуатации Системы.
- должны применяться средства АВЗ, сертифицированные по классификации ФСТЭК РФ.

Средства АВЗ должны обладать возможностью:

- отключения автоматического обновления и сканирования;
- отключения дополнительных функций АВЗ, за исключением файлового антивируса;
- обновления компонентов ПО и сигнатур вирусов только в «ручном» режиме;
- выполнения сканирования файловой системы только в «ручном» режиме;
- отключения автоматических действий с файлами (таких как их удаление, блокирование или перемещение). При обнаружении вредоносного ПО допускается только соответствующее оповещение на экран АРМ или сервера Системы со звуковым оповещением;
- анализа архивных, исполняемых файлов;
- запрета доступа к административным функциям АВЗ под любыми учетными записями, за исключением привилегированных. Доступ к настройкам АВЗ для учетных записей администраторов должен предоставляться только после ввода пароля доступа;
- исключения конкретных папок и файлов из области проверки средствами АВЗ для исключения негативного влияния на работоспособность компонентов Системы.

Для всех применяемых на АРМ и серверах Системы (коммутационные серверы, SCADA-системы, серверы приложений и БД) антивирусных средств обязательно официальное подтверждение поставщиком Системы и/или организацией, осуществляющей внедрение, техническую поддержку и/или сопровождение Системы, программной совместимости с ППО Системы.

7.7. ТРЕБОВАНИЯ К ПРЕДОТВРАЩЕНИЮ ВТОРЖЕНИЙ (КОМПЬЮТЕРНЫХ АТАК) (СОВ)

Требования не предъявляются, так как Системе присвоена категория значимости К3-3.

7.8. ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ЦЕЛОСТНОСТИ (ОЦЛ)

(ОЦЛ.0, ОЦЛ.1)

Для ОЦЛ в Системе должны выполняться меры:

- регламентация правил и процедур обеспечения целостности (ОЦЛ.0);
- контроль целостности ПО (ОЦЛ.1);

Данные меры должны быть реализованы за счёт использования встроенных в ППО и ОС механизмов защиты информации, разработки правил и процедур обеспечения целостности.

Общие требования к ОЦЛ:

В Системе и её СЗИ должна быть реализована возможность контроля целостности ПО, включая их обновления, с использованием контрольных сумм, хеш-функции или электронной подписи в процессе загрузки или динамически в процессе работы Системы.

Использование автоматизированных средств контроля состава и целостности ПО, при их наличии, не должно каким-либо образом влиять на работу ПО (блокировать или останавливать работу программ, удалять файлы), только регистрировать факт нарушения с указанием названия измененного программного модуля или не вошедшего в перечень разрешенного ПО.

7.9. ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ДОСТУПНОСТИ (ОДТ)

(ОДТ.0, ОДТ.4, ОДТ.5, ОДТ.6, ОДТ.8)

Для ОДТ в Системе должны выполняться меры:

- регламентация правил и процедур обеспечения доступности (ОДТ.0);
- резервное копирование информации (ОДТ.4);
- обеспечение возможности восстановления информации (ОДТ.5);
- обеспечение возможности восстановления ПО при нештатных ситуациях (ОДТ.6);
- контроль предоставляемых вычислительных ресурсов и каналов связи (ОДТ.8).

Данные меры должны быть реализованы за счёт использования встроенных в ОС, ППО механизмов защиты информации, СЗИ и средств резервного копирования, разработки правил и процедур обеспечения доступности.

Общие требования к ОДТ:

МЭ должны обладать возможностью конфигурирования в отказоустойчивом кластере.

Для обеспечения резервного копирования компонентов Системы, СЗИ, наряду со встроенными возможностями ОС, ППО Системы, должны применяться специализированные средства резервного копирования, включенные в состав СЗИ. СЗИ Системы должны обладать функциональной возможностью выполнения резервного копирования с сохранением резервных копий на машинные носители информации и сетевые ресурсы.

Должна быть обеспечена возможность просмотра/восстановления данных из резервных копий.

Резервному копированию подлежат:

- файлы и БД Системы и СЗИ – не реже одного раза в неделю;
- электронные журналы регистрации событий Системы – не реже одного раза в неделю;
- конфигурационные файлы компонентов Системы и СЗИ – при каждом внесении изменений в конфигурационные настройки Системы и её средств защиты, но не реже одного раза в месяц;
- образы системных жестких дисков АРМ, серверов Системы и СЗИ – не реже одного раза в месяц (неделя, в случае использования виртуальной инфраструктуры);

7.10. ТРЕБОВАНИЯ К ЗАЩИТЕ ТЕХНИЧЕСКИХ СРЕДСТВ И СИСТЕМ (ЗТС)

(ЗТС.0, ЗТС.2, ЗТС.3, ЗТС.4, ЗТС.5)

Для обеспечения ЗТС в Системе должны выполняться меры:

- регламентация правил и процедур защиты технических средств и систем (ЗТС.0);
- организация контролируемой зоны (ЗТС.2);
- управление физическим доступом (ЗТС.3);
- размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4);
- защита от внешних воздействий (ЗТС.5).

Данные меры защиты должны быть реализованы за счёт применения организационных и технических мер, разработки правил и процедур защиты технических средств и систем.

Общие требования к ЗТС:

Оборудование Системы (АРМ, сервера, АСО, МЭ, ПЛК, КИПиА) должно размещаться в запираемых шкафах, а также должно быть обеспечено пломбирование корпусов оборудования. В случае размещения в запираемых шкафах, в Системе должен быть реализован контроль доступа и оповещение оперативного персонала о вскрытии шкафа с последующей регистрацией события, с передачей в систему охранной сигнализации (при наличии технической возможности).

7.11. ТРЕБОВАНИЯ К ЗАЩИТЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ И ЕЕ КОМПОНЕНТОВ (ЗИС)

(ЗИС.0, ЗИС.1, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.21, ЗИС.34, ЗИС.35)

Для обеспечения ЗИС в Системе должны выполняться меры:

- регламентация правил и процедур защиты Системы и ее компонентов (ЗИС.0);
- разделение функций по управлению (администрированию) Системой с иными функциями (ЗИС.1);
- защита периметра Системы (ЗИС.2);
- эшелонированная защита Системы (ЗИС.3);
- организация ДМЗ (ЗИС.5);
- сокрытие архитектуры и конфигурации Системы (ЗИС.8);
- защита информации при ее передаче по каналам связи (ЗИС.19);
- обеспечение доверенных канала, маршрута (ЗИС.20);
- запрет несанкционированной удаленной активации периферийных устройств (ЗИС.21);
- защита от угроз отказа в обслуживании (DOS, DDOS-атак) (ЗИС.34);
- управление сетевыми соединениями (ЗИС.35)

Данные меры должны быть реализованы за счёт использования встроенных в ОС и ППО Системы механизмов защиты информации, АВЗ и МЭ, разработки правил и процедур защиты Системы и ее компонентов

Общие требования к ЗИС:

В Системе и её СЗИ должна быть реализована возможность локального либо с использованием защищенных протоколов сетевого взаимодействия администрирования и конфигурирования компонентов сетевой инфраструктуры Системы. Административный доступ должен быть разрешен только с сетевых адресов, специально выделенных для этого административных консолей.

Для снижения сложности администрирования при разграничении доступа к компонентам Системы необходима возможность реализации доступа, основанного на ролевом подходе. В соответствии с типовым уровнем полномочий для персонала Системы с одинаковыми должностными обязанностями формируется роль, основанная на принципе наименьших полномочий, необходимых для решения производственных задач.

При принятии решения о допустимости применения в промышленных сетях АСУТП / ИС систем беспроводной связи должна приниматься во внимание возможность блокирования беспроводной связи при использовании инженерно-технических средств защиты (например, средств радиоэлектронной борьбы с беспилотными летательными аппаратами) и должно обеспечиваться:

- выделение беспроводных сетей связи в отдельный сетевой сегмент с обеспечением его защиты с использованием МЭ;
- аутентификация беспроводных устройств при доступе к беспроводной сети с использованием криптографических алгоритмов;
- шифрование данных в каналах связи беспроводной сети с использованием криптографических алгоритмов.

7.12. ТРЕБОВАНИЯ К РЕАГИРОВАНИЮ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ (ИНЦ)

(ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, ИНЦ.6)

Для обеспечения ИНЦ в Системе должны выполняться меры:

- регламентация правил и процедур реагирования на компьютерные инциденты (ИНЦ.0);
- выявление компьютерных инцидентов (ИНЦ.1);
- информирование о компьютерных инцидентах (ИНЦ.2);
- анализ компьютерных инцидентов (ИНЦ.3);
- устранение последствий компьютерных инцидентов (ИНЦ.4);
- принятие мер по предотвращению повторного возникновения компьютерных инцидентов (ИНЦ.5);
- хранение и защита информации о компьютерных инцидентах (ИНЦ.6)

Данные меры должны быть реализованы за счёт использования встроенных в ОС, ППО механизмов, а также с помощью СЗИ, разработки правил и процедур реагирования на компьютерные инциденты.

Общие требования к ИНЦ:

В Системе и её СЗИ должна быть реализована возможность обнаружения и идентификации инцидентов ИБ, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, ПО и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов ИБ.

7.13. ТРЕБОВАНИЯ К УПРАВЛЕНИЮ КОНФИГУРАЦИЕЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ И ЕЕ СИСТЕМЫ ЗАЩИТЫ (УКФ)

(УКФ.0, УКФ.2, УКФ.3)

Для обеспечения УКФ в Системе должны выполняться меры:

- регламентация правил и процедур управления конфигурацией Системы (УКФ.0);
- управление изменениями (УКФ.2);
- установка (инсталляция) только разрешенного к использованию ПО (УКФ.3).

Данные меры должны быть реализованы за счёт использования встроенных в ОС, ППО механизмов защиты информации, АВЗ и МЭ, разработки правил и процедур управления конфигурацией Системы.

Общие требования к УКФ:

Встроенные механизмы защиты ППО, ОС, АВЗ и МЭ должны обладать возможностями:

- санкционирования внесения изменений в базовую конфигурацию Системы и ее СЗИ;
- регистрации действий по внесению изменений в базовую конфигурацию Системы и ее системы защиты;
- сохранения данных об изменениях базовой конфигурации Системы и ее системы защиты;

- контроля действий по внесению изменений в базовую конфигурацию Системы и ее системы защиты.

Конфигурация параметров Системы должна быть документирована.

Все действия по внесению изменений в конфигурацию Системы (изменения состава и параметров тегов, добавление/удаление оборудования, изменения в калибровочных/градуировочных таблицах, изменения алгоритмов работы Системы, изменения в параметрах защиты – изменение ролей и состава Пользователей, параметров аутентификации и пр.) должны регистрироваться в журналах регистрации Системы с указанием:

- даты и времени изменения;
- учетной записи Пользователя;
- названия и значения изменяемого параметра.

Для встроенного ПО (прошивок) контроллеров и микроконтроллеров должен поддерживаться файловый архив версий встроенного ПО с указанием истории вносимых изменений.

7.14. ТРЕБОВАНИЯ К УПРАВЛЕНИЮ ОБНОВЛЕНИЯМИ ПО (ОПО)

(ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4)

Для обеспечения ОПО в Системе должны выполняться меры:

- регламентация правил и процедур управления обновлениями ПО (ОПО.0);
- поиск, получение обновлений ПО от доверенного источника (ОПО.1);
- контроль целостности обновлений ПО (ОПО.2);
- тестирование обновлений ПО (ОПО.3);
- установка обновлений ПО (ОПО.4).

Данные меры должны быть реализованы за счёт использования встроенных в ОС, ППО механизмов защиты информации, АВЗ, МЭ и иных СЗИ, разработки правил и процедур управления обновлениями ПО.

Общие требования к ОПО:

В комплект поставки Системы должны входить инструкции по обновлению ОС, ППО, АВЗ, МЭ и иных СЗИ, а также регламенты (инструкции) по установке обновлений ОС, ППО, встроенного ПО от разработчика Системы.

7.15. ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ (ПЛН)

(ПЛН.0, ПЛН.1, ПЛН.2)

Для обеспечения ПЛН в Системе должны выполняться меры:

- регламентация правил и процедур планирования мероприятий по обеспечению защиты информации (ПЛН.0);
- разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации (ПЛН.1);
- контроль выполнения мероприятий по обеспечению защиты информации (ПЛН.2).

Данные меры должны быть реализованы за счет разработки правил и процедур планирования мероприятий по обеспечению защиты информации.

7.16. ОБЕСПЕЧЕНИЕ ДЕЙСТВИЙ В НЕШТАТНЫХ СИТУАЦИЯХ (ДНС)

(ДНС.0, ДНС.1, ДНС.2, ДНС.5)

Для обеспечения ДНС в Системе должны выполняться меры:

- регламентация правил и процедур обеспечения действий в нештатных ситуациях (ДНС.0);
- разработка плана действий в нештатных ситуациях (ДНС.1);
- обучение и отработка действий персонала в нештатных ситуациях (ДНС.2);
- обеспечение возможности восстановления Системы в случае возникновения нештатных ситуаций (ДНС.5);

Данные меры должны быть реализованы за счёт использования встроенных в ОС, ППО механизмов защиты информации, МЭ, разработки правил и процедур обеспечения действий в нештатных ситуациях.

Общие требования к ДНС:
В дополнение к указанным мерам защиты информации для обеспечения действий в нештатных (непредвиденных) ситуациях (ДНС) необходимо учитывать меры защиты информации и обязательные дополнительные функциональные возможности Системы и её СЗИ для обеспечения доступности (ОДТ).

7.17. ИНФОРМИРОВАНИЕ И ОБУЧЕНИЕ ПЕРСОНАЛА (ИПО)

(ИПО.0, ИПО.1, ИПО.2, ИПО.4)

Для обеспечения ИПО в Системе должны выполняться меры:

- регламентация правил и процедур информирования и обучения персонала (ИПО.0);
- информирование персонала об угрозах безопасности информации и о правилах безопасной работы (ИПО.1);
- обучение персонала правилам безопасной работы (ИПО.2);
- контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы (ИПО.4).

Данные меры должны быть реализованы за счёт разработки правил и процедур информирования и обучения персонала.

7.18. ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ КИПиА СИСТЕМЫ

Программируемые компоненты КИПиА и СИ должны иметь парольную защиту от несанкционированного доступа к просмотру и изменению настроек и конфигурации, а также изменению технологических параметров средства измерения.

Метрологически значимое ПО, включая микропрограммное обеспечение оборудования КИПиА, должно быть защищено от несанкционированного доступа, иметь идентификационные данные, подтверждаемые при проведении испытаний в целях утверждения типа СИ. При использовании в качестве идентификационных данных CRC32 обязательно указание криптографически стойкой хеш-суммы из ряда MD5, SHA1, ГОСТ 34.11).

Команды и данные, введенные через интерфейс Пользователя оборудования КИПиА и СИ, не должны оказывать недопустимое влияние на метрологически значимое ПО и данные. Должно быть предусмотрено однозначное назначение каждой команды для инициирования функции или изменения данных в соответствии с сопроводительной технической документацией.

Конструкция оборудования КИПиА и СИ должна обеспечивать ограничение доступа к определенным частям СИ (включая ПО), в целях предотвращения несанкционированных настройки и вмешательства, которые могут привести к искажениям результатов измерений.

Защита ПО и данных в оборудовании КИПиА и ИС должна быть обеспечена в соответствии с ГОСТ Р 8.654-2015.

В эксплуатационной документации на оборудование КИПиА и СИ должны быть описаны:

- все интерфейсы, посредством которых возможно изменение метрологически значимых параметров средства измерения, а также средства контроля доступа к указанным интерфейсам (в том числе фактов использования конфигурационного ПО);
- возможности независимой, т.е. выполняемой сторонним ПО, проверки идентификационных данных (контрольной суммы CRC32, MD5, SHA1 или специально разработанный алгоритм с указанием способа их вычисления) микропрограммного обеспечения средства измерения, а также метрологически значимой части ПО для подтверждения подлинности ПО.

7.19. ТРЕБОВАНИЯ К ОБОСНОВАНИЮ ДОСТАТОЧНОСТИ ПРИНЯТЫХ МЕР ЗАЩИТЫ И ПРИМЕНЕНИЮ КОМПЕНСИРУЮЩИХ МЕР

При отсутствии возможности реализации отдельных мер защиты информации на каком-либо из уровней Системы и (или) невозможности их применения к отдельным объектам и субъектам доступа, в том числе вследствие их негативного влияния на штатный режим функционирования Системы, Подрядной организацией должны быть предложены иные СЗИ с представлением документального обоснования их применимости либо разработаны компенсирующие меры, обеспечивающие адекватное блокирование (нейтрализацию) угроз ИБ и необходимый уровень защищенности Системы с учётом присвоенного класса защищённости / категории значимости Системы и актуальной модели угроз ИБ.

В ходе разработки СЗИ Системы и в проектной документации должно быть приведено обоснование применения компенсирующих мер защиты информации, а при приемочных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз ИБ.

.

8. ТРЕБОВАНИЯ К РАЗДЕЛЕНИЮ КОРПОРАТИВНЫХ И ПРОМЫШЛЕННЫХ СЕТЕЙ

Промышленные сети Системы должны быть логически или физически выделены в отдельный сетевой сегмент. При этом:

- точки доступа в сеть Системы из других сетей связи должны быть минимальны и документированы, в том числе с указанием резервных точек доступа при выходе из строя основных;
- устройство, обеспечивающее сегментацию и фильтрацию сетевых соединений между сетью Системы и прочими сетями связи, должно быть настроено на запрет любых сетевых соединений, кроме явно разрешенных;
- правила фильтрации сетевых соединений с сетью Системы должны обеспечивать фильтрацию на основе сетевых адресов, портов и прикладных протоколов.

Для предоставления данных из сети Системы в сети смежных или вышестоящих систем (MES, ERP) должен быть реализован подход по размещению серверов с данными Системы (серверы отчетов, серверы БД реального времени, серверы с историческими данными параметров технологических процессов, сообщений и сигнализации) в отдельной промежуточной сети промышленной ДМЗ.

Не разрешается использовать для разделения корпоративной и промышленной сетей рабочие станции с двумя сетевыми картами (dual-homed), за исключением случая, когда функционал МЭ является их единственным задействованным функционалом.

Альтернативой использованию МЭ при организации периметральной защиты сетей Системы является применение технологий однонаправленной передачи для информационного взаимодействия с информационными системами уровня ОГ (MES-системы): однонаправленных шлюзов или дата-диодов. При этом, помимо повышенной сетевой безопасности за счет исключения возможности компьютерных атак со стороны зоны с меньшим уровнем безопасности, достигается значительное упрощение построения и обслуживания сетевой защиты периметра.

Все сервисы, необходимые Системе, должны быть размещены в пределах промышленной сети или промышленной ДМЗ (AD, серверы АВЗ и обновлений и т.д.). При сбоях МЭ, а также в целях предотвращения компьютерной атаки, МЭ должен иметь возможность перехода в режим полной блокировки трафика через границу промышленной сети.

9. ТРЕБОВАНИЯ К ПРОГРАММНОМУ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ СИСТЕМЫ И ОТДЕЛЬНЫМ СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

9.1. ТРЕБОВАНИЯ К ПЕРИМЕТРАЛЬНЫМ СРЕДСТВАМ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

Межсетевое экранирование является основным механизмом обеспечения защиты и сегментации промышленных сетей Системы.
Средства МЭ должны удовлетворять следующим функционально-техническим требованиям:

- гибкая гранулярная система распределения прав администраторов – от прав только на чтение определенных данных одного домена управления МЭ до мультидоменного администратора с полными правами на весь функционал;
- аутентификация и авторизация доступа пользователей к системе управления должна осуществляться как встроенными средствами самой системой управления МЭ, так и иметь возможность использования внешних систем, включающих, но не ограничивающихся такими как, RADIUS, TACACS;
- возможность как централизованного, так и локального управления МЭ;
- обеспечение резервного копирования конфигурации ПО МЭ (встроенные средства резервного копирования);
- возможность отключения логирования для отдельных правил политики МЭ;
- фильтрация трафика на основе политики межсетевого экранирования с использованием технологии Stateful Inspection. Возможность обработки трафика транспортных протоколов в режимах stateless и stateful;
- возможность работы в режиме моста (на 2-ом уровне модели OSI, bridge);
- возможность осуществлять NAT: NAT, PAT, Static NAT;
- маршрутизация на основе политик, PBR;
- агрегация каналов в пассивном режиме объединение по стандарту 802.3ad;
- функционал IDS/IPS должен быть интегрирован в МЭ;
- поддержка отказоустойчивой кластеризации;
- МЭ в кластерном исполнении должен поддерживать обновление ПО без влияния на трафик, который он обрабатывает;
- операционная система МЭ должна иметь модуль контроля основных показателей функционирования всех программных слоёв системы и программно-аппаратной платформы для интеграции с внешними системами мониторинга через протокол SNMP версии не ниже 3 при помощи snmp-запросов и snmp-ловушек (trap). Включая, но не ограничиваясь такими как:
  - должен иметь мониторинг статуса интерфейсов;
  - должен иметь мониторинг загрузки использования процессора, памяти, дискового пространства;
  - должен иметь мониторинг сессий TCP, UDP;
  - должен иметь мониторинг packets accept-rate, drop rate, syn-flood-rate;
  - должен иметь мониторинг состояния кластера;
  - должен иметь простой интерфейс для написания скриптов – скрипты расширенного мониторинга, управления конфигурациями, инвентаризации и т.п.
- аудит действий привилегированных пользователей на уровне приложения, бизнес логики, ОС;

- МЭ должен иметь встроенную систему мониторинга своих основных параметров, таких как CPU, RAM, климатических показателей, состояние дисков, количество подключений, состояние сетевой статистики в реальном времени.
- глубокая инспекция протоколов (в том числе промышленных), с целью регулирования и фильтрации трафика, а также накопления статистических данных;
- контроль целостности программной части МЭ;

Конфигурация МЭ, установленных между сетями Системы и прочими сетями ОГ, а также МЭ промышленных сетей связи должна отвечать следующим требованиям:

- прямое сетевое взаимодействие Системы со сторонними сетями запрещено; взаимодействие должно осуществляться через сегмент промышленной ДМЗ;
- должны быть запрещены любые соединения, кроме явно разрешенных;
- входящие сетевые соединения в сеть Системы из прочих сетей ОГ могут осуществляться только через промышленную ДМЗ;
- порты и сервисы между корпоративными сетями и сетями Системы предоставляются на индивидуальной основе под конкретный случай. Обоснованием должна служить согласованная с ИБ ОГ заявка на открытие порта или сервиса;
- все правила политик безопасности МЭ должны содержать сетевые адреса (группы адресов) или идентификаторы (группы идентификаторов) источников и назначений сетевых соединений, порты и протоколы;
- должен быть разрешен минимально необходимый исходящий трафик из сетей Системы. Например, только для предоставления данных технологических процессов на серверы исторических данных и отчетов, к OPC-интерфейсам.

Для защиты сетевой инфраструктуры Системы от несанкционированного доступа на периметре промышленной сети рекомендуется применение МЭ, сертифицированных по требованиям безопасности информации в соответствии с информационным сообщением ФСТЭК РФ «Об утверждении Требований к межсетевым экранам» от 28.04.2016 № 240/24/1986 для системы 3 категории значимости – МЭ, соответствующие 6 классу защиты.

Администрирование и конфигурирование МЭ должно осуществляться с локальной консоли, доступ к которой физически ограничен, либо с использованием защищенных протоколов сетевого взаимодействия. Административный доступ к МЭ должен быть разрешен только с сетевых адресов специально выделенных для этого рабочих станций.

При выборе средств МЭ следует в приоритетном порядке учитывать рекомендации Компании и производителя Системы.

9.2. ТРЕБОВАНИЯ К СРЕДСТВАМ АКТИВНОГО СЕТЕВОГО ОБОРУДОВАНИЯ

АСО должно размещаться в защищенных помещениях, в запираемых шкафах. Логический доступ к любому АСО должен предоставляться только после успешного прохождения процедур идентификации. Все порты и сетевые интерфейсы, не используемые в ходе эксплуатации оборудования, должны быть отключены или опечатаны.

Удаленное управление АСО должно осуществляться при выполнении следующих условий:

- осуществляется безопасная идентификация и аутентификация администраторов с использованием криптографической защиты аутентификационных данных;
- применен защищенный протокол (HTTPS и др.);
- используются фиксированные сетевые адреса;
- производится обязательная регистрация всех событий входа, а также вводимых администраторами команд в журналах регистрации.

Все соединения с АСО должны быть защищены паролем.

Консольные порты АСО должны отключаться после установленного периода неактивности.

На всём АСО должны быть отключены все неиспользуемые сервисы и должна быть включена регистрация событий. В обязательном порядке должны регистрироваться события:

- доступ администраторов к АСО;
- действия администраторов, включая внесение изменений в конфигурации;
- установка обновлений;
- ошибки и сбои в работе оборудования;
- сетевые события, такие как результат попытки установления соединения, результаты аутентификации, включение и отключение каналов связи и пр.

Хранение журналов регистрации должно осуществляться на выделенном сервере.

Для быстрого восстановления конфигурации АСО сети Системы ее резервные копии должны быть сохранены на соответствующих носителях.

Средства АСО, применяемые для защиты на втором уровне Системы, должны удовлетворять следующим техническим и функциональным характеристикам:

- VLAN:
  - группы VLAN;
  - 802.1Q Tagged VLAN;
  - VLAN на основе порта;
  - 802.1v Protocol VLAN;
  - VLAN на основе MAC-адресов;
  - VLAN Trunking.
- безопасность:
  - SSH v2;
  - SSL v1/v2/v3;
  - Port Security;
  - привязка IP-MAC-Port;
  - поддержка протокола SNMP v3;

- контроль целостности ПО и файлов конфигурации по контрольным суммам;
- защита от широковещательного/многоадресного/одноадресного шторма;
- сегментация трафика.

9.3. ТРЕБОВАНИЯ К ИСТОЧНИКАМ БЕСПЕРЕБОЙНОГО ПИТАНИЯ

Все активное серверное и сетевое оборудование и СЗИ должно обеспечиваться ИБП.
ИБП должны обладать следующими техническими и функциональными требованиями:

- в случае сбоя постоянного источника электропитания должен обеспечить работоспособность технических СЗИ Системы не менее 45 минут;
- должна быть предусмотрена предупредительная сигнализация о необходимости замены аккумулятора;
- должна быть предусмотрена визуальная и звуковая сигнализация нештатного состояния;
- должен быть предусмотрен механизм автоматического включения зарядного устройства ИБП при восстановлении подачи электроснабжения;
- должна быть предусмотрена возможность контроля и управления ИБП через ЛВС с использованием протокола SNMP v3;
- должна быть предусмотрена возможность отключения неиспользуемых сетевых протоколов.

Надежность электроснабжения СЗИ Системы должна соответствовать требованиям нормативных и технических документов к устройству электроустановок, относимых к особой группе энергоприемников первой категории.

9.4. ТРЕБОВАНИЯ К ПРОГРАММНО-ТЕХНИЧЕСКИМ СРЕДСТВАМ

Программно-технические средства Системы должны обладать следующими возможностями:

- отключение всех служб и сервисов на АРМ и серверах управления Системы, не используемых в процессе эксплуатации и сопровождения Системы (при наличии технической возможности). При необходимости данные службы, сервисы и функции должны иметь возможность включения на определенный период времени в соответствии с требованиями по управлению конфигурацией Системы;
- отключение или блокировка всех коммуникационных портов, портов ввода-вывода и интерфейсы на оборудовании Системы, включая АРМ, серверов управления, коммуникационного оборудования, не используемых в процессе эксплуатации и сопровождения Системы;
- запрет загрузки ОС с иных носителей, кроме жесткого диска компьютеров и серверов, в BIOS АРМ операторов и инженерных станций и серверов управления Системы, ограничение паролем доступа к внесению изменений параметров BIOS;
- документирование безопасной конфигурации параметров Системы и её СЗИ.

9.5. ТРЕБОВАНИЯ К ПРИКЛАДНОМУ ПО СИСТЕМЫ

ППО, планируемое к внедрению в рамках создания Системы и обеспечивающее выполнение его функций по назначению, должно соответствовать следующим требованиям по безопасности:

9.5.1. Требования по безопасной разработке ПО

- наличие руководства по безопасной разработке ПО;
- проведение анализа угроз безопасности информации ПО.

9.5.2. Требования к испытаниям по выявлению уязвимостей в ПО

- проведение статического анализа исходного кода программы;
- проведение фаззинг-тестирования программы, направленного на выявление в ней уязвимостей.

9.5.3. Требования к поддержке безопасности ПО

- наличие процедур отслеживания и исправления обнаруженных ошибок и уязвимостей ПО;
- определение способов и сроков доведения разработчиком (производителем) ПО до его пользователей информации об уязвимостях ПО, о компенсирующих мерах по защите информации или ограничениях по применению ПО, способов получения пользователями обновлений ПО, проверки их целостности и подлинности.

В качестве граничных маршрутизаторов, имеющих доступ к информационно-телекоммуникационной сети "Интернет", выбираются маршрутизаторы, сертифицированные на соответствие требованиям по безопасности информации (в части реализованных в них функций безопасности). В случае отсутствия технической возможности применения граничных маршрутизаторов, сертифицированных на соответствие требованиям по безопасности информации, функции безопасности граничных маршрутизаторов подлежат оценке на соответствие требованиям по безопасности в рамках приемки или испытаний Системы. Обоснование отсутствия технической возможности приводится в проектной документации на Систему (СЗИ Системы).

9.6. ТРЕБОВАНИЯ К СРЕДСТВАМ, ПРЕДНАЗНАЧЕННЫМ ДЛЯ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

Планируемые к установке средства, предназначенные для обнаружения, предупреждения ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты в ОГ, должны быть согласованы с ФСБ РФ через корпоративный центр ГосСОПКА.

10. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ СИСТЕМЫ И ЕЁ СЗИ

В рамках обеспечения требований законодательства, нормативно-правовых актов РФ (приказ ФСТЭК РФ от 14.03.2014 № 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 ФСТЭК РФ от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации») и ЛНД Компании в области ИБ – основные проектные решения, комплекты проектной, конструкторской и рабочей документации Системы должны быть дополнены разделами по ИБ.

Требования ЛНД Компании по обеспечению ИБ АСУТП и защите объектов КИИ должны быть учтены на всех этапах создания/модернизации Системы.

Разделы по обеспечению ИБ Системы, реализуемой наложенными СЗИ, могут быть оформлены в виде отдельных томов с дополнениями в качестве ссылок на разделы соответствующих томов документации на Систему, с описанием встроенных СЗИ. Перечень проектной конструкторской и эксплуатационной документации по обеспечению ИБ Системы должен соответствовать перечню документов, приведенному в Таблице ТТИБ_1

Таблица ТТИБ_1
Перечень документов по обеспечению ИБ Системы

СОСТАВ ПРОЕКТНОЙ, КОНСТРУКТОРСКОЙ И РАБОЧЕЙ (ЭКСПЛУАТАЦИОННОЙ) ДОКУМЕНТАЦИИ ПО ОБЕСПЕЧЕНИЮ ИБ СИСТЕМЫ	
№ ПП	**НАИМЕНОВАНИЕ ДОКУМЕНТА**
1	Разработка проектной документации по ИБ Системы в составе:
1.1	Частное ТЗ по обеспечению ИБ Системы
1.2	Модель угроз ИБ Системы
1.3	Акт классификации / категорирования Системы
1.4	Сведения о категорировании Системы (неполные)
1.5	Пояснительная записка по ИБ в составе (допускается общая с Системой):
1.5.1	Схема функциональной структуры
1.5.2	Схема структурная КТС
1.5.3	Описание КТС
1.5.4	Спецификация оборудования и ПО, включая формирование разделительной ведомости, уточнение Проектно-сметной документации
2	Конструкторская документация в части ИБ в составе:
2.1	Пояснительная записка
2.2	Структурная и функциональная схемы
2.3	Спецификация
2.4	Программа и методика испытаний
2.5	Паспорт/Формуляр
2.6	Руководство пользователя
2.7	Руководство администратора
2.8	Регламент предоставления доступа
2.9	Регламент непрерывности функционирования
2.10	Регламент внесения изменений в конфигурацию
3	Рабочая документация в составе:

3.1	Спецификация (при наличии)
3.2	Схема структурная КТС
3.3	Схема функциональной структуры
3.4	Чертежи установки технических средств
3.5	Локальный сметный расчет
3.6	Схема соединения внешних проводок
3.7	Схема подключения внешних проводок
3.8	План расположения
3.9	Перечень заданий на разработку смежных разделов, связанных с созданием Системы (строительных)
3.10	Задания на разработку смежных разделов, связанных с созданием Системы (строительных)
3.11	Копии протоколов испытаний, содержащие результаты оценки соответствия СЗИ
3.12	Список установленного ПО на АРМах и серверах Системы
3.13	Список запущенных служб
3.14	Межсетевые взаимодействия с указанием протоколов и правила обмена
3.15	Список критических файлов с проверкой целостности (с указанием контрольных сумм и способов их проверки)
3.16	Схема сети АСУТП с указанием (IP адресов , DNS-имен, сетевых взаимодействий на уровне портов и протоколов.)
3.17	Описание запущенных процессов (системных и SCADA-системы)
3.18	Указание конфигурации АСО (активного сетевого оборудования), при наличии такового
3.19	Указание настройки межсетевых экранов (при их наличии) в виде правил взаимодействия
3.20	Карта сети с указанием потоков движения информации и используемых протоколов.
4	Исполнительная документация в составе:
4.1	Сведения о Системе при подключении к сетям общего пользования
5	Разрешительная документация в части ИБ
5.1	Заключенный Договор по присоединению к сетям связи общего пользования

Допускается расширение перечня документов, требуемых для описания ИБ Системы. Конкретный перечень необходимых документов должен быть приведен при разработке и согласовании частного ТЗ на СЗИ Системы.

Разработка ОРД, регламентирующей правила и процедуры обеспечения ИБ Системы, осуществляется на этапе внедрения организационных и технических мер по обеспечению безопасности Системы в соответствии с рекомендациями Компании, проектной, конструкторской и рабочей (эксплуатационной) документацией на Систему и корректируется до ввода Системы в промышленную эксплуатацию на этапах опытной эксплуатации и проведения анализа уязвимостей Системы и её СЗИ.

10.2. ОБЪЕМ ПОСТАВКИ СЗИ

Поставщик СЗИ должен иметь лицензию ФСТЭК РФ на деятельность по технической защите конфиденциальной информации на соответствующие виды работ и услуг согласно требованиям постановления Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

План СМР на Систему должен включать требования по обеспечению ИБ.

В случае поставки (передачи) криптографических СЗИ необходима лицензия ФСБ РФ на соответствующие виды работ и услуг в рамках требований постановления Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

Поставщик должен предложить Систему, созданную на базе серийно выпускаемых современных технических средств и последних версий базового ПО.

Гарантийный срок на СЗИ Системы должен составлять не менее 24 месяцев, с момента передачи в промышленную эксплуатацию или 36 месяцев от даты отгрузки.

Поставка прикладного ПО должна включать в себя установочные дистрибутивы, лицензионные ключи/пароли.

Укрупненный перечень оборудования СЗИ Системы приведен в Таблице ТТИБ_2.

Таблица ТТИБ_2
Объем поставки СЗИ

№ П/П	НАИМЕНОВАНИЕ	КОЛИЧЕСТВО
1	2	3
	СЗИ Системы, в составе:	
1	Средства АВЗ рабочих станций и серверов:	
1.1	Kaspersky Industrial Cyber Security for Nodes	*
2	Средства резервного копирования:	
2.1	Кибер-Бэкап	*
3	Средства периметральной защиты МЭ	*

*количество будет уточнено на этапе проектирования.

10.3. СТРОИТЕЛЬНО-МОНТАЖНЫЕ РАБОТЫ ПО СОЗДАНИЮ ПОДСИСТЕМЫ ИБ

СМР выполняется подрядчиком по отдельному договору, данные ТТ выполнение СМР не предполагают.

10.4. ШЕФ-МОНТАЖНЫЕ И ПУСКОНАЛАДОЧНЫЕ РАБОТЫ ПО ОБЕСПЕЧЕНИЮ ИБ

На стадии организации пусконаладочных работ календарный план, согласно проекту производства работ, должен включать требования по обеспечению ИБ.

Перечень пусконаладочных и инжиниринговых работ по обеспечению ИБ приведен в Таблице ТТИБ_3 «Перечень ПНР и ИР по ИБ», перечень указан справочно и может быть дополнен при необходимости.

Таблица ТТИБ_3
Перечень ПНР и ИР по обеспечению ИБ

№ П/П	НАИМЕНОВАНИЕ РАБОТ
1	2
1	**Проведение автономной наладки СЗИ**
1.1	Проверка комплектности поставки проектной документации СЗИ
1.2	Подключение электропитания на компоненты СЗИ
1.3	«Холодный» пуск оборудования СЗИ
1.4	Визуальная проверка индикаторов состояния СЗИ
1.5	Визуальная проверка работоспособности компонентов оборудования
2	**Проведение автономной наладки МЭ**
2.1	Подключение МЭ
2.2	Загрузка ПО в МЭ
2.3	Активация и настройка функций МЭ (IPS, IPsec VPN, NAT и др.)
2.4	Настройка IP адресации портов МЭ
2.5	Разработка, согласование правил (политик) фильтрации МЭ
2.6	Перевод МЭ в прозрачный режим
2.7	Анализ трафика в прозрачном режиме
2.8	Отключение неиспользуемых портов, сервисов
2.9	Отладка работы МЭ
2.10	Внесение правил фильтрации в МЭ
2.11	Перевод МЭ в штатный режим работы
3	**Проведение автономной наладки АВЗ**
3.1	Установка ОС
3.2	Базовая настройка ОС
3.3	Установка ПО централизованного управления АВЗ
3.4	Настройка ПО централизованного управления АВЗ
3.5	Разработка политик, задач безопасности антивирусного ПО
3.6	Настройка политик, задач безопасности антивирусного ПО
3.7	Автономная проверка ППО АВЗ совместно с представителями заказчика
3.8	Установка ПО АВЗ на АРМ

№ П/П	НАИМЕНОВАНИЕ РАБОТ
1	2
3.9	Настройка ПО АВЗ на АРМ
4	**Проведение автономной наладки сервера резервного копирования:**
4.1	Установка ОС
4.2	Базовая настройка ОС
4.3	Установка ПО централизованного управления резервным копированием
4.4	Настройка ПО централизованного управления резервным копированием
4.5	Разработка политик, задач резервного копирования
4.6	Настройка политик, задач резервного копирования
4.7	Автономная проверка резервного копирования ППО СЗИ совместно с представителями заказчика
5	**Настройка АСО**
5.1	Установка ПО
5.2	Конфигурирование коммутатора
5.3	Отключение неиспользуемых портов, сервисов
5.4	Настройка правил коммутации
5.5	Установка и базовая настройка средства сбора событий
5.6	Установка и базовая настройка средства управления МЭ
6	**Настройка встроенных СЗИ в соответствии с требованиями Компании**
7	**Проведение комплексной наладки СЗИ**
7.1	Проверка связи компонентов СЗИ. Наладка, устранение неисправностей
7.2	Проверка взаимодействия компонентов СЗИ совместно с представителями заказчика
7.3	Наладка СЗИ в соответствии с требованиями настоящего документа

10.5. ПЕРЕЧЕНЬ ОТЧЕТНЫХ ДОКУМЕНТОВ ПО ПРИЕМКЕ СЗИ

Отчетные документы по приемке СЗИ разрабатывается в соответствии с требованиями СП 77.13330.2016, Положения Компании «Формирование приемо-сдаточной документации на объектах строительства Компании».

Перечень отчетных документов по приемке СЗИ приведен в Таблице ТТИБ_4:

Таблица ТТИБ_4
Перечень отчетных документов по приемке СЗИ

№ П/П	НАИМЕНОВАНИЕ ДОКУМЕНТА
1	2
1	Общий журнал работ
2	Акт проверки СЗИ
3	Акт передачи оборудования, изделий и материалов (СЗИ) в монтаж
4	Акт приемки смонтированных СЗИ
5	Программа и методика автономных испытаний СЗИ, утвержденная заказчиком
6	Протоколы проведения автономных испытаний (приложения к Акту приемки индивидуальных испытаний)
7	Акт приемки СЗИ после автономных испытаний
8	Программа и методика комплексных испытаний СЗИ, утвержденная заказчиком
9	Протоколы проведения комплексных испытаний (приложения к Акту комплексного опробования)
10	Акт комплексного опробования СЗИ
11	Принятие решения о возможности эксплуатации Системы и её СЗИ
12	Акт о приемке СЗИ в опытную эксплуатацию
13	Акт о завершении опытной эксплуатации СЗИ
14	Паспорт на оборудование, руководства по эксплуатации, разрешения на применение (при необходимости), сертификаты соответствия и др. заводская документация на СЗИ.
15	Решение о возможности (или невозможности) проведения приемочных испытаний Системы и её СЗИ
16	Акт приемо-сдаточных испытаний на предприятиях-изготовителях комплектов СЗИ в соответствии с Перечнем оборудования, подлежащих заводской приемке с участием представителей заказчика*
17	Положительное заключение (вывод) в акте приемки (или аттестате соответствия) о соответствии Системы установленным требованиям по обеспечению безопасности
18	Акт о приемке СЗИ в постоянную эксплуатацию

*<u>Примечание</u>: * Применимо в случае поставки СЗИ в виде изделия полной заводской готовности.*

10.6. ПОРЯДОК ПРОВЕДЕНИЯ ИСПЫТАНИЙ СЗИ

Испытания СЗИ проводятся с учетом ГОСТ Р 59792-2021 по готовности к испытаниям объекта защиты Системы, а также требований ЛНД Компании и законодательства РФ в области ИБ.

Для СЗИ устанавливаются следующие основные виды испытаний:

- предварительные испытания;
- опытная эксплуатация;
- приемочные испытания.

Предварительные испытания СЗИ включают проверку его работоспособности, оценку влияния СЗИ на функционирование Системы при проектных режимах работы, установленных проектной документацией, а также принятие решения о возможности опытной эксплуатации СЗИ.

Предварительные испытания на объекте заказчика проводятся Подрядной организацией, выполняющей ПНР по программе и методике, разработанной поставщиком и утвержденной заказчиком.

Опытная эксплуатация СЗИ включает проверку функционирования СЗИ, в том числе реализованных организационных и технических мер защиты информации, а также готовность персонала Системы к эксплуатации СЗИ.

Опытная эксплуатация СЗИ производится силами заказчика по утвержденной программе и методике, разработанной поставщиком, при участии Подрядной организации, выполнившей ПНР.

Приемочные испытания СЗИ проводятся в рамках комплексных приемочных испытаний Системы при полностью развернутых и настроенных СЗИ.

В ходе приемочных испытаний СЗИ должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие СЗИ утвержденному ТЗ на создание (модернизацию) Системы и (или) ТЗ (частному ТЗ) на создание СЗИ.

Результаты приемочных испытаний СЗИ отражаются в общем акте приемки Системы в эксплуатацию.

11. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ ПРЕДВАРИТЕЛЬНЫХ ИСПЫТАНИЙ СИСТЕМЫ И ЕЁ СЗИ

Предварительные испытания Системы и её СЗИ проводятся для определения работоспособности и решения вопроса о возможности приемки Системы и её СЗИ в опытную эксплуатацию. Предварительные испытания следует выполнять после проведения разработчиком отладки и тестирования поставляемых программных и технических средств Системы и её СЗИ и представления им соответствующих документов о их готовности к испытаниям, а также после ознакомления персонала Системы с эксплуатационной документацией.

Перечень отчетных документов по проведению предварительных испытаний Системы и её СЗИ приведен в таблице ТТИБ_5.

Предварительные испытания Системы и её СЗИ должны проводиться в соответствии с программой и методиками предварительных испытаний и включать проверку работоспособности СЗИ Системы, оценку выполнения требований по безопасности, предъявляемых к программным и программно-аппаратным средствам, в том числе СЗИ, в соответствии с пунктами 27 - 31 Приказа ФСТЭК РФ от 25.12.2017 № 239, оценку влияния СЗИ на функционирование Системы при проектных режимах его работы, установленных проектной документацией, а также принятие решения о возможности опытной эксплуатации Системы и её СЗИ.

Таблица ТТИБ_5
Перечень отчетных документов по проведению предварительных испытаний СЗИ

№ П/П	НАИМЕНОВАНИЕ ДОКУМЕНТА
1	2
1	Программа и методика предварительных испытаний Системы и её СЗИ
2	Акт о завершении предварительных испытаний Системы и её СЗИ
3	Принятие решения о возможности опытной эксплуатации Системы и её СЗИ

12. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ ОПЫТНОЙ ЭКСПЛУАТАЦИИ СИСТЕМЫ И ЕЁ СЗИ

Опытная эксплуатация Системы и её СЗИ должна проводиться в соответствии с программой и методиками опытной эксплуатации и включать проверку функционирования СЗИ Системы, в том числе реализованных организационных и технических мер, а также знаний и умений пользователей и администраторов, необходимых для эксплуатации Системы и её СЗИ. По результатам опытной эксплуатации принимается решение о возможности (или невозможности) проведения приемочных испытаний Системы и её СЗИ.

Перечень отчетных документов по проведению опытной эксплуатации Системы и её СЗИ приведен в таблице ТТИБ_6.

Таблица ТТИБ_6
Перечень отчетных документов по проведению опытной эксплуатации Системы и её СЗИ

№ П/П	НАИМЕНОВАНИЕ ДОКУМЕНТА
1	2
1	Программа и методика опытной эксплуатации Системы и её СЗИ
2	Акт о завершении опытной эксплуатации Системы и её СЗИ
3	Решение о возможности (или невозможности) проведения приемочных испытаний Системы и её СЗИ

13. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ АНАЛИЗА УЯЗВИМОСТЕЙ СИСТЕМЫ

Анализ уязвимостей Системы проводится в целях выявления недостатков (слабостей) в СЗИ Системы и оценки возможности их использования для реализации угроз ИБ. При этом анализу подлежат уязвимости кода, конфигурации и архитектуры Системы.

Анализ уязвимостей проводится для всех программных и программно-аппаратных средств Системы и её СЗИ. При проведении анализа уязвимостей применяются следующие способы их выявления:

- анализ проектной, рабочей (эксплуатационной) документации и организационно-распорядительных документов по безопасности Системы;
- анализ настроек программных и программно-аппаратных средств Системы и её СЗИ;
- выявление известных уязвимостей программных и программно-аппаратных средств, посредством анализа состава, установленного ПО и обновлений безопасности с применением средств контроля (анализа) защищенности и (или) иных СЗИ;
- выявление известных уязвимостей программных и программно-аппаратных средств, сетевых служб, доступных для сетевого взаимодействия, с применением средств контроля (анализа) защищенности;
- тестирование на проникновение в условиях, соответствующих возможностям нарушителей, определенных в модели угроз ИБ.

Применение способов и средств выявления уязвимостей осуществляется субъектом КИИ с учетом особенностей функционирования Системы.
Допускается проведение анализа уязвимостей на макете (в тестовой зоне) Системы или макетах отдельных сегментов Системы.

Анализ уязвимостей Системы проводится до ввода её в эксплуатацию на этапах, определяемых субъектом КИИ.

В случае выявления уязвимостей Системы, которые могут быть использованы для реализации (способствовать возникновению) угроз ИБ, принимаются меры, направленные на их устранение или исключающие возможность использования (эксплуатации) нарушителем выявленных уязвимостей.
По результатам анализа уязвимостей должно быть подтверждено, что в Системе отсутствуют уязвимости, как минимум содержащиеся в банке данных угроз ИБ ФСТЭК РФ, или выявленные уязвимости не приводят к возникновению угроз ИБ в отношении Системы.

По результатам анализа угроз ИБ могут быть разработаны рекомендации по корректировке архитектуры Системы и ОРД по безопасности Системы, направленные на блокирование (нейтрализацию) отдельных угроз ИБ.

Перечень отчетных документов по проведению анализа уязвимостей Системы приведен в таблице ТТИБ_7.

Таблица ТТИБ_7
Перечень отчетных документов по проведению анализа уязвимостей Системы

№ П/П	НАИМЕНОВАНИЕ ДОКУМЕНТА
1	2
1	Результаты анализа проектной, рабочей (эксплуатационной) документации и организационно-распорядительных документов по безопасности Системы.
2	Результаты анализа настроек программных и программно-аппаратных средств Системы и её СЗИ.
3	Результаты выявления известных уязвимостей программных и программно-аппаратных средств.
4	Результаты тестирования на проникновение.
5	Результаты устранения или исключения возможности использования (эксплуатации) нарушителем выявленных уязвимостей.
6	Рекомендации по корректировке архитектуры Системы
7	Рекомендации по корректировке ОРД по безопасности Системы
6	Акт о завершении анализа уязвимостей Системы, и его результаты.

14. ТРЕБОВАНИЯ К ПРИЕМОЧНЫМ ИСПЫТАНИЯМ СИСТЕМЫ И ЕЁ СЗИ

В ходе приемочных испытаний Системы и её СЗИ должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие Системы и её СЗИ настоящим требованиям, а также требованиям ТЗ на создание Системы и (или) ТЗ (частного ТЗ) на создание СЗИ.

В качестве исходных данных при приемочных испытаниях используются:

- модель угроз ИБ, которая должна поддерживаться в актуальном состоянии в процессе функционирования Системы в соответствии с методическими рекомендациями ФСТЭК РФ;
- результаты (акт) категорирования;
- техническое задание на создание (модернизацию) Системы и (или) ТЗ (частное ТЗ) на создание СЗИ;
- проектная и рабочая (эксплуатационная) документация на Систему;
- ОРД по безопасности Системы;
- результаты анализа уязвимостей Системы;
- материалы предварительных испытаний и опытной эксплуатации;
- иные документы, разрабатываемые в соответствии с настоящими требованиями и требованиями стандартов организации.

Приемочные испытания Системы и ее СЗИ проводятся в соответствии с программой и методикой приемочных испытаний. Результаты приемочных испытаний Системы и ее СЗИ с выводом о ее соответствии установленным требованиям включаются в акт приемки Системы в эксплуатацию.
Ввод в эксплуатацию Системы и ее СЗИ осуществляется при положительном заключении (выводе) в акте приемки (или в аттестате соответствия) о соответствии Системы установленным требованиям по обеспечению ИБ.
По итогам ввода Системы и её СЗИ в промышленную эксплуатацию формируются полные сведения для дальнейшего направления регулятору для учета.