

Приложение № 2
к документации о закупке

Договор №
возмездного оказания услуг

г. Барнаул

2026г.

Общество с ограниченной ответственностью «БАРНАУЛЬСКИЙ ВОДОКАНАЛ» (ООО «БАРНАУЛЬСКИЙ ВОДОКАНАЛ») в лице Генерального директора Полуго Андрея Сергеевича, действующего на основании Устава, с одной стороны, именуемое в дальнейшем «Заказчик»,
и _____, «_____», именуемое в дальнейшем «Исполнитель», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», заключили настоящий Договор (именуемый в дальнейшем «Договор») о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

- 1.1. Исполнитель обязуется качественно и на высоком профессиональном уровне оказывать услуги в объеме согласно Заданию Заказчика, изложенному в Приложении № 1, являющемуся неотъемлемой частью настоящего Договора, а Заказчик обязуется принять оказанные услуги и оплатить их.
- 1.2. Объем и сроки оказания Исполнителем услуг, могут быть изменены по обоюдному письменному согласию Сторон, с одновременным изменением размера вознаграждения и соблюдением законодательства о закупках.

2. СРОКИ ОКАЗАНИЯ УСЛУГ

- 2.1. Исполнитель оказывает услуги в период с даты подписания договора до «15» декабря 2027 года.
- 2.2. Сроки оказания конкретных видов услуг по настоящему Договору определены в Приложении № 1.
- 2.3. За нарушение сроков оказания Услуг Заказчик вправе потребовать с Исполнителя уплаты неустойки в размере 0,1 % от общей стоимости Услуг за каждый день просрочки.

3. ОБЯЗАННОСТИ СТОРОН

3.1. Обязанности Исполнителя:

3.1.1. Исполнитель проинформирован о возможном наличии на Объекте пропускного и внутриобъектового режимов. До начала выполнения работ на Объекте Исполнитель должен получить у Заказчика информацию о порядке и условиях соблюдения пропускного и внутриобъектового режимов». До начала выполнения работ Исполнитель обязан обратиться к Заказчику и получить у Заказчика информацию о наличии на Объекте пропускного и внутриобъектового режимов. При наличии действующих на Объекте пропускного и внутриобъектового режимов Исполнитель обязан ознакомиться с порядком и условиями пропускного и внутриобъектового режимов и обеспечить их соблюдение. При получении от Заказчика согласия на привлечение соисполнителя (-ей) Исполнитель обязан сообщить Заказчику информацию о привлеченных соисполнителях и ознакомить работников привлеченных соисполнителей с порядком и условиями соблюдения пропускного и внутриобъектового режимов».

3.1.2. Надлежащим образом лично выполнить услуги, предусмотренные пунктом 1.1 настоящего Договора, и в случае необходимости привлекать по письменному согласованию с Заказчиком других высококвалифицированных специалистов (при этом Исполнитель обязуется обеспечить выполнение указанными специалистами условий настоящего Договора и несет ответственность перед Заказчиком за действия указанных специалистов).

Исполнитель обязуется привлечь соисполнителя (-ей) из числа СМСП, указанных им в плане привлечения соисполнителей из числа СМСП. При этом общая стоимость обязательств, выполненных соисполнителями из числа СМСП, должна составлять не менее 25 % от стоимости Договора, указанной в п. 4.1 Договора. *(условие исключается в случае заключения Договора с Исполнителем из числа СМСП или в случае отсутствия в ДоЗ требования о привлечении соисполнителей из числа СМСП).*

За неисполнение/ненадлежащее исполнение обязательства, предусмотренного настоящим пунктом Договора в части доли привлечения Исполнителем соисполнителей из числа СМСП (если такое условие предусмотрено Договором), Исполнитель оплачивает Заказчику штраф в размере, в котором им не исполнена обязанность по привлечению к исполнению Договора соисполнителей из числа СМСП

согласно плана привлечения соисполнителей из числа СМСП, в течение 7 рабочих дней с даты исполнения Договора.

3.1.3. Информировать Заказчика о ходе оказания услуг, представлять Заказчику для подписания универсального передаточного документа (УПД) не позднее последнего числа каждого месяца или по окончании оказания услуг, если предусмотрено Приложением № 1;

3.1.4. в своей деятельности руководствоваться интересами Заказчика;

3.1.5. исполнять свои обязательства по настоящему Договору в сроки, предусмотренные настоящим Договором.

3.1.6. Исполнитель обязан иметь и предъявлять Заказчику по его требованию в течение 3 (трех) рабочих дней все сертификаты, лицензии, разрешения и прочие документы, удостоверяющие правомерность Исполнителя оказывать услуги в соответствии с законодательством РФ и настоящим Договором.

3.1.7. выставить универсальный передаточный документ или иной аналогичный документ, если это предусмотрено налоговым законодательством и по форме, утвержденной соответствующим компетентным государственным органом. За не выставление такого документа Заказчик может потребовать уплаты Исполнителем штрафа в размере процентной ставки НДС от общей суммы указанного документа с НДС.

3.1.8. В случае если Приложением № 1 в рамках оказания услуг по настоящему Договору предусмотрена поставка товара, для которого указан номер реестровой записи из реестра российской промышленной продукции, из евразийского реестра промышленных товаров государств-членов Евразийского экономического союза, из единого реестра российских программ для электронных вычислительных машин и баз данных или из единого реестра программ для электронных вычислительных машин и баз данных из государств-членов Евразийского экономического союза, то не допускается поставка товара с другим номером реестровой записи из вышеуказанных реестров или товара, отсутствующего в вышеуказанных реестрах. Если в рамках оказания услуг подлежит поставке товар, происходящий из Российской Федерации или из стран ЕАЭС, то не допускается замена его на товар, происходящий из иностранного государства.

3.2. Обязанности Заказчика:

3.2.1. Обеспечивать Исполнителя по его запросу всей информацией, документами и материалами, необходимыми для выполнения данных последнему поручений, предусмотренных пунктом 1.1 настоящего Договора, перечень и срок предоставления которых предварительно согласовывается Сторонами;

3.2.2. При обращении Исполнителя к Заказчику за информацией о наличии на Объекте пропускного и внутриобъектового режимов и условиях их соблюдения, Заказчик должен в минимально возможные сроки ознакомить Исполнителя с требованиями пропускного и внутриобъектового режимов и порядком их соблюдения.

3.2.3. Своевременно оплачивать оказанные услуги Исполнителя в соответствии с условиями статьи 4 настоящего Договора.

4. ПОРЯДОК РАСЧЕТОВ

4.1. Стоимость услуг за весь объем услуг по настоящему Договору составляет _____ (_____) рублей, кроме того НДС по ставке, установленной действующим законодательством Российской Федерации.

Указанная стоимость услуг по настоящему Договору включает в себя любые расходы, понесенные Исполнителем для оказания услуг по настоящему Договору.

4.2. Оплата услуг по договору (отдельному этапу договора) производится в рублях на основании подписываемого сторонами универсального передаточного документа в течение 7 рабочих дней с момента его подписания.

4.3. При оплате стоимости услуг Заказчик вправе приостановить исполнение обязательства по оплате оказанных услуг в случае нарушения Исполнителем сроков оказания услуг или других обязательств, предусмотренных условиями настоящего договора, в целях определения размера штрафов и/или неустоек, предусмотренных условиями настоящего Договора.

4.4. В случае начисления Исполнителю штрафов и/или неустоек в порядке и размере, установленном настоящим договором, при оплате стоимости услуг Заказчик вправе в одностороннем порядке произвести удержание части денежных средств, тем самым уменьшив стоимость оплаты по договору. В этом случае размер оплаты оказанных услуг уменьшается на сумму удержания, рассчитанную в соответствии с условиями настоящего Договора.

5. КОНФИДЕНЦИАЛЬНОСТЬ

5.1. При исполнении своих обязательств по настоящему Договору каждая из Сторон в порядке и на условиях, предусмотренных настоящим Договором, вправе в случаях, предусмотренных законодательством, передать информацию, составляющую ее коммерческую тайну либо персональные данные ее работников (далее - Информация), другой Стороне (далее - Получающая Сторона), а Получающая Сторона обязана использовать полученную Информацию в порядке и на условиях, предусмотренных настоящим Договором.

5.2. Исполнитель («Получающая Сторона») согласен считать конфиденциальной информацией всю информацию, которая передается ему Заказчиком («Раскрывающая Сторона»). К конфиденциальной информации также следует относить информацию об исполняемых Получающей Стороной услугах. Получающая Сторона обязуется использовать конфиденциальную информацию Раскрывающей Стороны исключительно в рамках исполнения своих обязательств по настоящему Договору. Исполнитель обязуется принять все необходимые меры по обеспечению конфиденциальности, в том числе предусмотренные Федеральным законом от 29 июля 2004 г. N98-ФЗ "О коммерческой тайне" в отношении предмета Договора, хода его исполнения, полученных результатов, включая мероприятия по охране документации и материалов, ограничению круга лиц, допущенных к информации и заключению с ними Соглашений о конфиденциальности. Передача Заказчиком Исполнителю документации, информации, составляющей коммерческую тайну и других конфиденциальных сведений, осуществляется в порядке, установленном положениями настоящего договора о конфиденциальности. Если в ходе выполнения предусмотренных Договором услуг Исполнитель привлекает третьих лиц, которым для оказания услуг необходим доступ к конфиденциальным сведениям, Исполнитель обязан заключить с указанными третьими лицами соответствующие Соглашения о конфиденциальности.

5.3. Информация Стороны (далее - Раскрывающая Сторона), может быть предоставлена Получающей Стороне, уполномоченным ею лицам в устной форме, или путем предоставления доступа к документам, содержащим Информацию, или путем передачи документов, содержащих Информацию.

5.4. По каждому факту предоставления доступа к документам, содержащим Информацию, или передачи документов, содержащих Информацию Получающей Стороне Сторонами непосредственно после предоставления доступа к документам, содержащим Информацию, или передачи документов, содержащих Информацию должен подписываться Акт в двух экземплярах (по одному для каждой из Сторон). По каждому факту предоставления Информации в устной форме должен подписываться Протокол встречи.

5.5. Вся Информация, составляющая коммерческую тайну, передаваемая в письменной форме, должна быть помечена грифом «Коммерческая тайна» с указанием Раскрывающей Стороны (ее реквизитов).

5.6. Получающая Сторона должна соблюдать строгую конфиденциальность в отношении Информации, не разглашать, не копировать, не воспроизводить и не передавать Информацию любому третьему лицу, не использовать Информацию в целях, отличных от предусмотренных настоящим Договором.

5.7. Получающая Сторона имеет право передать Информацию третьим лицам при условии предварительного письменного согласия на это Раскрывающей Стороны. За действия третьих лиц по соблюдению конфиденциальности в отношении Информации отвечает Получающая Сторона.

5.8. Получающая Сторона вправе предоставить органам государственной власти страны, резидентом которой является Получающая Сторона, Информацию без предварительного письменного согласия Раскрывающей Стороны Информации только в случаях, когда это прямо предусмотрено законодательством страны, резидентом которой является Получающая Сторона, в отношении этих органов. В таких случаях Получающая Сторона обязана:

- предпринять все разумные усилия для уведомления Раскрывающей Стороны до момента раскрытия такой Информации о предполагаемой форме, сроке, характере и цели такого раскрытия, или (если это невозможно) уведомить Раскрывающую Сторону обо всех обстоятельствах такого раскрытия незамедлительно после такого раскрытия;
- не позднее дня, следующего за днем получения Получающей Стороной от органов государственной власти страны, резидентом которой она является, запроса (требования), в том числе устного, о предоставлении Информации, предоставить полную информацию об этом запросе (требовании), в том числе его копию, Раскрывающей Стороне;
- не позднее дня, следующего за днем предоставления Получающей Стороной органам государственной власти страны, резидентом которой она является, Информации предоставить Раскрывающей Стороне полный перечень Информации, предоставленной этим органам государственной власти.

5.9. Требования настоящего Договора в отношении Информации прекращают действовать:

- через 5 (пять) лет со дня подписания уполномоченными представителями Сторон последнего Акта или Протокола встречи по отношению ко всем подписанным Сторонами соответственно Актам или Протоколам встреч;

- по заключении Сторонами соглашения, содержащего положения, заменяющие положения настоящего Договора в отношении Информации; или
- по письменному согласованию Сторон.

5.10. Получающая Сторона обязана в течение 5 (пяти) календарных дней со дня прекращения действия, в том числе расторжения, по какой-либо причине настоящего Договора, или при получении в любое время письменного запроса Раскрывающей Стороны; или принятия решения о реорганизации или ликвидации Раскрывающей Стороны уничтожить или передать Раскрывающей Стороне все имеющиеся у Получающей Стороны документы или любые другие материалы, содержащие Информацию, в том числе копии таких материалов и удалить Информацию из любых носителей данных, в том числе компьютеров или другой аппаратуры, содержащей Информацию.

5.11. Раскрывающая Сторона имеет право получить документальное подтверждение уничтожения Информации, надлежащим образом заверенное уполномоченным лицом Получающей Стороны, контролирующим этот процесс.

6. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРОВ

6.1. Настоящий Договор регулируется и толкуется в соответствии с законодательством Российской Федерации.

6.2. Все споры и разногласия, которые могут возникнуть в процессе исполнения Сторонами своих обязательств по настоящему Договору, будут по возможности решаться путем переговоров. Но в случае направления претензии, стороны согласовали, что она может быть направлена через оператора посредством электронного документооборота. Если Стороны не придут к согласию путем переговоров, то спор передается в суд в соответствии с действующим законодательством Российской Федерации.

7. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ (ФОРС-МАЖОР)

7.1. Стороны не несут ответственности за неисполнение любого из своих обязательств, если докажут, что такое неисполнение было вызвано форс-мажорными обстоятельствами, т.е. событиями или обстоятельствами, действительно находящимися вне контроля такой Стороны, наступившими после заключения настоящего Договора, носящими непредвиденный и непредотвратимый характер. К форс-мажорным обстоятельствам относятся, в частности, природные катаклизмы, забастовки, пожары, наводнения, взрывы, обледенения, войны (как объявленные, так и необъявленные), мятежи, гибель товара, задержки перевозчиков, вызванные авариями или неблагоприятными погодными условиями, опасности и случайности на море, эмбарго, катастрофы, ограничения, налагаемые государственными органами (включая распределения, приоритеты, официальные требования, квоты и ценовой контроль), если эти обстоятельства непосредственно повлияли на исполнение настоящего Договора.

7.2. Время, которое требуется Сторонам для исполнения своих обязательств по настоящему Договору, будет продлено на любой срок, в течение которого было отложено исполнение по причине перечисленных обстоятельств.

7.3. В случае если продолжительность обстоятельств форс-мажора превышает 30 дней, настоящий Договор может быть расторгнут по письменному заявлению любой из сторон.

7.4. Несмотря на наступление форс-мажора, перед прекращением настоящего Договора вследствие форс-мажорных обстоятельств Стороны осуществляют окончательные взаимные расчеты.

7.5. Сторона, для которой стало невозможным исполнение обязательств по настоящему Договору по причине наступления форс-мажорных обстоятельств, должна незамедлительно информировать другую Сторону в письменном виде о возникновении вышеуказанных обстоятельств, а также в течение 30 дней предоставить другой Стороне подтверждение форс-мажорных обстоятельств. Таким подтверждением будет являться справка, сертификат или иной соответствующий документ, выданный уполномоченным государственным органом, расположенным по месту возникновения форс-мажорных обстоятельств.

7.6. Стороны пришли к соглашению, что никакие меры или ограничения, принятые или установленные государственными, муниципальными, международными органами, должностными лицами, организациями или учреждениями в рамках защиты здоровья населения и/или противодействия распространению коронавирусной инфекции (COVID-19), иных заболеваний, представляющих опасность для окружающих, принятие решений о проведении военных операций, специальных военных операций, иных военных, антитеррористических и иных подобных действий (объявленных и не объявленных), не могут считаться препятствием к исполнению настоящего Договора, не признаются обстоятельством непреодолимой силы для целей настоящего Договора, не являются основанием для освобождения Сторон от ответственности за неисполнение или ненадлежащее исполнение обязательств по настоящему Договору, а также не являются основанием для расторжения и/или изменения

настоящего Договора полностью или в части по требованию какой-либо из Сторон Договора.

8. ТРЕБОВАНИЯ В ОБЛАСТИ ОХРАНЫ ТРУДА, ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ И ОХРАНЫ ОКРУЖАЮЩЕЙ СРЕДЫ

8.1. В ходе оказания услуг по настоящему Договору Исполнитель обязуется:

8.1.1. соблюдать нормы действующего законодательства Российской Федерации, включая законодательство о недрах, об охране окружающей среды, о промышленной и пожарной безопасности, иные законы и нормативные акты, действующие на территории оказания услуг;

8.1.2. обеспечить выполнение необходимых мероприятий по промышленной безопасности, охране труда, охране окружающей среды, рациональному использованию природных ресурсов, по пожарной безопасности объекта, на котором оказываются услуги;

8.1.3. соблюдать внутренние нормативные документы Заказчика в области охраны труда, промышленной безопасности и охраны окружающей среды.

8.1.4. соблюдать требования к оборудованию, используемому в ходе оказания услуг по настоящему Договору и его эксплуатации, установленные действующим законодательством РФ.

8.2. Исполнитель самостоятельно несет ответственность за допущенные им при оказании услуг нарушения природоохранного, водного, земельного, лесного законодательства, законодательства в области пожарной безопасности, охраны труда, атмосферного воздуха, опасных производственных объектов и т.д., включая оплату штрафов, пеней, а также по возмещению причиненного в связи с этим вреда. В случае если Заказчик был привлечен к ответственности за вышеуказанные нарушения Исполнителя, последний обязуется возместить Заказчику все причиненные этим убытки.

8.3. При наличии вины Исполнителя за аварии, инциденты и несчастные случаи, произошедшие в процессе работы, последний обязуется возместить Заказчику причиненные убытки.

8.4. Заказчик не несет ответственности за травмы, увечья или смерть Исполнителя, произошедшие не по вине Заказчика, а также в случае нарушения Исполнителем правил техники безопасности или промышленной санитарии.

8.5. Заказчик вправе в любое время осуществлять контроль за соблюдением Исполнителем и третьими лицами, привлекаемыми Исполнителем, положений настоящей статьи Договора. Обнаруженные в ходе проверки нарушения фиксируются в акте, подписываемом представителями Заказчика, Исполнителем. В случае отказа Исполнителя от подписания такого акта, он оформляется Заказчиком в одностороннем порядке.

8.6. Несоблюдение Исполнителем требований настоящей статьи является существенным нарушением условий настоящего Договора и дает Заказчику право требовать уплаты штрафа в размере 1 000 рублей за каждый случай нарушения, а также расторгнуть настоящий Договор в одностороннем порядке без обязательств Заказчика по возмещению убытков Исполнителя, связанных с таким расторжением.

9. АНТИАЛКОГОЛЬНАЯ ОГОВОРКА

9.1. Исполнитель не вправе оказывать услуги по настоящему Договору в состоянии алкогольного, наркотического или токсического опьянения.

9.2. Исполнитель обязан не допускать пронос и нахождение на территории Заказчика веществ, вызывающих алкогольное, наркотическое или токсическое опьянение, за исключением веществ, необходимых для осуществления производственной деятельности на территории Заказчика (далее - «Разрешенные вещества»).

9.3. В целях обеспечения контроля за указанными ограничениями Заказчик имеет право производить проверки и досмотр всех транспортных средств, вещей и материалов, доставляемых Исполнителем на территорию Заказчика. Если в результате подобного досмотра будут обнаружены указанные запрещенные вещества, то Исполнитель не допускается на территорию Заказчика.

9.4. В случае обнаружения на территории Заказчика Исполнителя в состоянии алкогольного, наркотического или токсического опьянения, проноса или нахождения на территории Объекта веществ, вызывающих алкогольное, наркотическое или токсическое опьянение, за исключением Разрешенных веществ, Исполнитель уплачивает Заказчику штраф в размере _____ рублей за каждый такой факт.

9.5. Фиксация факта появления Исполнителя на территории Заказчика в состоянии алкогольного, наркотического или токсического опьянения, проноса или нахождения на территории Заказчика веществ, вызывающих алкогольное, наркотическое или токсическое опьянение, за исключением Разрешенных веществ, для целей настоящего Договора и отношений между Заказчиком и Исполнителем может осуществляться любым из нижеперечисленных способов:

- медицинским осмотром, или
- освидетельствованием;
- актами, составленными работниками Заказчика (контрагентами Заказчика);
- письменными объяснениями работников Заказчика (контрагентов Заказчика);
- другими способами.

9.6. Заказчик имеет право в любое время проверять исполнение Исполнителем обязанностей, предусмотренных в настоящем разделе Договора. В случае возникновения у Заказчика подозрения о наличии на территории Заказчика Исполнителя в состоянии опьянения, Исполнитель обязан по требованию Заказчика незамедлительно прекратить оказание услуг на территории Заказчика.

10. АНТИКОРРУПЦИОННАЯ ОГОВОРКА

10.1. При исполнении своих обязательств по Договору, Стороны, их аффилированные лица, работники или посредники не выплачивают, не предлагают выплатить и не разрешают выплату каких-либо денежных средств или ценностей, прямо или косвенно, любым лицам, для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества и иные неправомерные цели.

10.2. При исполнении своих обязательств по Договору, Стороны, их аффилированные лица, работники или посредники не осуществляют действия, квалифицируемые применимым для целей Договора законодательством, как дача/получение взятки, коммерческий подкуп, а также действия, нарушающие требования применимого законодательства и международных актов о противодействии легализации (отмыванию) доходов, полученных преступным путем.

10.3. В случае возникновения у Стороны подозрений, что произошло или может произойти нарушение каких-либо положений настоящей Статьи, соответствующая Сторона обязуется уведомить другую Сторону в письменной форме. После письменного уведомления, соответствующая Сторона имеет право приостановить исполнение обязательств по Договору до получения подтверждения, что нарушения не произошло или не произойдет. Это подтверждение должно быть направлено в течение десяти рабочих дней с даты направления письменного уведомления.

10.4. В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений настоящей Статьи контрагентом, его аффилированными лицами, работниками или посредниками, выражающееся в действиях, квалифицируемых применимым законодательством, как дача или получение взятки, коммерческий подкуп, а также действиях, нарушающих требования применимого законодательства и международных актов о противодействии легализации доходов, полученных преступным путем.

10.5. В случае нарушения одной Стороной обязательств воздерживаться от запрещенных в настоящем разделе Договора действий и/или неполучения другой Стороной в установленный Договором срок подтверждения, что нарушения не произошло или не произойдет, другая Сторона имеет право расторгнуть Договор в одностороннем порядке полностью или в части, направив письменное уведомление о расторжении. Сторона, по чьей инициативе был расторгнут Договор в соответствии с положениями настоящей статьи, вправе требовать возмещения реального ущерба, возникшего в результате такого расторжения.

11. ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

11.1. Документы, которыми Стороны обмениваются в электронном формате, подписываются Усиленной квалифицированной электронной подписью (УКЭП) уполномоченных лиц обеих Сторон соглашения. Каждая из Сторон может иметь несколько уполномоченных лиц для обмена информацией в рамках Договора. Каждое уполномоченное лицо должно иметь собственную электронную подпись, сертифицированную в установленном порядке в соответствии с нормами Федерального закона №63-ФЗ, и доверенность (МЧД), подтверждающую полномочия этого лица, оформленную Стороной в установленном порядке (при необходимости). Виды документов, которыми Стороны обмениваются в рамках настоящего Договора:

11.2. Формализованные ЭД – электронные документы, для которых нормативно-правовыми актами РФ установлены обязательные и (или) рекомендованные электронные форматы. На момент заключения настоящего Соглашения Стороны согласовали обмен в электронном формате следующих формализованных электронных документов:

- ✓ универсальный передаточный документ (УПД), в том числе корректировочный и на аванс;
- ✓ акт сверки взаимных расчетов с контрагентами;

✓ транспортная накладная.

11.3. Неформализованные ЭД – электронные документы, для которых нормативно-правовыми актами РФ не установлены обязательные и (или) рекомендованные электронные форматы:

✓ договоры, соглашения, дополнительные соглашения, в том числе дополнительные соглашения к договорам, ранее подписанных на бумажных носителях собственноручной подписью; приложения к ним;

✓ корреспонденция, а также, любая переписка, осуществляемая Сторонами в рамках договоров/соглашений/дополнительных соглашений (в том числе в порядке досудебного урегулирования спора), в том числе направление претензий

✓ соглашения о конфиденциальности (коммерческой тайне), Соглашение об электронном документообороте и иные виды соглашений;

✓ иные документы, конкретизирующие условия договоров/соглашений и подтверждающие выполнение операций кроме документов, для которых утвержден обязательный формат или которые передаются исключительно на бумажных носителях;

✓ документы о передаче имущественных прав (за исключением случаев, когда для соответствующих целей Стороны используют формализованные ЭД), акты МХ-1, акты МХ-3;

✓ наряд-заказы, акты наладки (испытаний, ввода в эксплуатацию), акты установления гарантийного срока, иные виды и формы актов и проектно-техническая документация для которых законодательными актами РФ не предусмотрен обмен в рекомендованных или обязательных электронных форматах;

✓ счета на оплату.

11.4. Форматы обмена электронными документами:

11.4.1 Обмен формализованными документами осуществляется в формате XML, PDF. Представление таких документов осуществляется автоматически Оператором ЭДО.

11.4.2. Обмен неформализованными документами преимущественно осуществляется в формате PDF – акты, письма, счет на оплату. Для документов, содержащих большой объем данных, изначально оформленных не в текстовых редакторах, допускается обмен документов в формате MS Excel.

11.4.3. Электронный обмен документами осуществляется через Операторов ЭДО, внесенных в Реестр доверенных операторов юридически значимого электронного документооборота, в соответствии с нормативно-правовым актом, утвержденным государственным органом, уполномоченным осуществлять правовое регулирование Операторов ЭДО.

11.5. Стороны согласились осуществлять ЭДО через следующих Операторов ЭДО:

➤ Заказчик – ООО «Компания «Тензор»», ИНН 7605016030, Идентификатор доверенного ОЭД 2ВЕ, обеспечивающее обмен информацией по телекоммуникационным каналам связи и фиксирующее факт и дату направления и получения информации в рамках электронного документооборота компании;

➤ Исполнитель – наименование «_____», ИНН _____, Идентификатор ОЭД _____.

11.6. В случае осуществления обмена документами через различных операторов ЭДО, Заказчик инициирует настройку роуминга между операторами.

11.7. Применяя электронный документооборот, Стороны руководствуются действующим законодательством РФ.

11.8. Стороны договорились соблюдать следующие правила при обмене первичными учетными документами:

11.8.1. Комплект (контейнер) документов должен включать универсальный передаточный документ.

11.8.2. Один комплект документов (контейнер) может содержать только 1 экземпляр универсального передаточного документа.

11.8.3. Комплект (контейнер) документов, кроме универсального передаточного документа может включать дополнительные документы, обосновывающие/детализирующие выполнение работ/услуг, поставку товаров. Обмен дополнительными документами производится в формате PDF в соответствии с п. 11.3. Договора.

11.8.4. В один комплект документов (контейнер) должны быть включены первичные учетные документы только по одной хозяйственной операции.

11.8.5. Производить обмен Актами сверки взаимных расчетов отдельными комплектами документов (контейнерами), без первичных учетных документов и подтверждающих документов.

11.8.6. Не допускается передача первичных учетных документов одной хозяйственной операции в электронном и бумажном форматах.

11.8.7. Не допускается наличие на документе, переданном через Оператора ЭДО, рукописных подписей и печатей контрагента за исключением служебных отметок о согласовании документов на дополнительных документах, подтверждающих выполнение операции.

11.9. Стороны осуществляют обмен электронными машиночитаемыми доверенностями (МЧД) путем включения идентификационного номера МЧД уполномоченного лица в штамп (оттиск) электронной подписи, размещенного на PDF-представлении электронного документа, или путем включения контейнера подписанной МЧД в контейнер электронных первичных учетных документов, которыми обмениваются Стороны.

11.10. Стороны не осуществляют обмен документами о купле-продаже товаров и документами о передаче результатов услуг (документ об оказании услуг) в электронном виде в неформализованном формате. Стороны осуществляют обмен универсальным передаточным документом, формат которого ФНС России.

11.11. Распечатанные электронные документы признаются сторонами дубликатами и не обладают равной юридической силой с электронными документами.

11.12. Стороны обязаны информировать друг друга о невозможности обмена документами в электронном виде, подписанными УКЭП, в частности:

- в случае технического сбоя на стороне программного обеспечения Сторон или Оператора ЭДО;
- в случае несвоевременного обновления ключей ЭП и квалифицированных сертификатов.

В период, когда обмен ЭД невозможен или осложнен, Стороны производят обмен документами на бумажном носителе подписанными собственноручной подписью.

ЭДО между Сторонами не отменяет обмен документами, не относящимися к первичной учетной документации в бумажном формате.

11.13. Стороны признают, что электронный документ, заверенный действующей на момент передачи электронной подписью (ЭП), является эквивалентом идентичного по содержанию документа на бумажном носителе, подписанного уполномоченным лицом Стороны с проставлением печати, имеет равную с ним юридическую силу и порождает для Сторон соответствующие права и обязанности.

11.14. Электронный документ порождает обязательства Стороны по Договору и Соглашению с момента постановки электронной подписи (ЭП), если он заверен действующей электронной подписью (ЭП) уполномоченного Стороной лица. При этом содержание электронного документа должно соответствовать полномочиям лица, его подписавшего.

11.15. Стороны признают, что используемые средства подготовки, передачи и проверки электронных документов достаточны для обеспечения надежного, эффективного и безопасного документооборота.

11.16. Стороны признают используемую в электронном документообороте систему защиты информации достаточной для защиты от несанкционированного доступа, контроля целостности передаваемых данных, а также подтверждения авторства и подлинности электронных документов.

11.17. Взаимные обязанности и права Сторон:

- обеспечить антивирусную безопасность и оперативную ликвидацию вирусных программ, разрушающих систему электронного документооборота, операционную систему и прочие программные средства с компьютеров, на которых установлено программное обеспечение для обмена электронными документами и подписания их ЭП;
- каждая из Сторон имеет право запрашивать и обязана по запросам другой Стороны направлять в течение 5-и рабочих дней с момента получения запроса надлежащим образом оформленные бумажные копии электронных документов, обмен которыми проходил в электронном цифровом виде;
- каждая из Сторон несет ответственность за своевременное обновление ключей и сертификатов, обеспечение конфиденциальности ключей ЭП, недопущение использования принадлежащих ей ключей без ее согласия;

Стороны не позднее 10 (десяти) рабочих дней с момента заключения настоящего Соглашения и в дальнейшем не позднее, чем за 10 (десять) рабочих дней до истечения срока действия ЭП, обязуются за свой счет получать ключи ЭП и сертификаты.

11.18. Стороны обязаны уведомлять друг друга обо всех случаях компрометации ключей ЭП о прекращении или об изменении полномочий лиц, указанных в настоящем Договоре, а также об изменении их адресов электронной почты в течение 3 (трех) календарных дней с момента такого изменения.

12. ПРАВА НА РЕЗУЛЬТАТЫ РАБОТ

12.1. Права на все результаты работ, включая исключительные права на результаты интеллектуальной деятельности (далее – РИД), в том числе на изобретения, полезные модели, промышленные образы, секреты производства, программы для ЭВМ, базы данных и иные произведения, права на получения патентов, права на все материальные объекты (отчетная, конструкторская, технологическая, рабочая документация, экспериментальное оборудование,

экспериментальные и опытные образцы и иные материальные объекты), созданные в ходе исполнения обязательств по настоящему Договору, с момента их создания, возникновения в полном объеме принадлежат Заказчику вне зависимости от того, было ли их создание прямо предусмотрено Договором. Заказчику принадлежат исключительные права на все результаты, не ограниченные во времени, месте либо содержании, на использование в любом виде результатов, которые были произведены в рамках Договора, в том числе (но не ограничиваясь):

- а) право на воспроизведение;
- б) право на публичный показ;
- в) право на практическую реализацию;
- г) право на доработку и изменение, в том числе его передачу для доработки (изменения) третьим лицам.

12.2. Исполнитель не вправе использовать для собственных нужд РИД и иные материальные объекты, созданные в рамках Договора.

12.3. Исполнитель гарантирует, что им надлежащим образом урегулированы все отношения с авторами РИД. Все расчеты с авторами РИД, созданных по настоящему договору и/или вошедших в состав РИД, созданных по настоящему договору (использованных Исполнителем при создании РИД), произведены Исполнителем самостоятельно и за свой счет. Исполнитель обязан предоставить Заказчику полную информацию об авторах и/или иных обладателях интеллектуальных прав на РИД и/или РИД, составной частью вошедшие в РИД, созданных по настоящему договору (использованных Исполнителем при создании РИД).

12.4. Исполнитель дает Заказчику согласие на использование РИД без указания своего имени (наименования), имен авторов РИД или иных правообладателей, если такие имеются (анонимное использование РИД). Исполнитель гарантирует, что получил от обладателей исключительных прав на РИД, разрешение на использование Заказчиком РИД, без указания имени или наименования (анонимно). Заказчик по своему усмотрению вправе использовать РИД анонимно либо указывать Исполнителя или иных авторов РИД.

12.5. Вознаграждение за создание, отчуждение прав на РИД и иные материальные объекты, прав на получение патентов входит в общую цену, предусмотренную условиями настоящего Договора. Вознаграждение является фиксированным и единоразовым, включающим в себя все возможные издержки и затраты Исполнителя, которые он может понести при исполнении своих обязательств, включая, но не ограничиваясь только этим, выплату любых видов вознаграждения авторам и иным правообладателям. Никакие дополнительные отчисления в пользу Исполнителя и/или иных авторов и правообладателей от использования Заказчиком любого созданного РИД и материального объекта не выплачиваются.

12.6. Стороны договорились о том, что к настоящему Договору не применяется право на удержание, предусмотренного ст. ст. 359, 360 ГК РФ. Исполнитель ни при каких обстоятельствах не имеет права удерживать результаты, в том числе РИД и иные материальные объекты, полученное в ходе исполнения настоящего Договора и обязан передать их Заказчику.

12.7. Исполнитель дает Заказчику согласие на создание любых производных произведений, в том числе на внесение в РИД изменений, сокращений и дополнений, на включение в состав сложных объектов или составного произведения. Исполнитель дает Заказчику согласие на обнародование РИД.

12.8. Ответственность за нарушение исключительных, личных неимущественных и иных прав третьих лиц при выполнении обязательств по данному Договору полностью возлагается на Исполнителя. В случае предъявления к Заказчику требований, претензий, исков, связанных с использованием созданных Исполнителем результатов, в том числе РИД и иных материальных объектов, Исполнитель обязан урегулировать их собственными силами и за свой счет. Доказанные убытки, которые могут возникнуть у Заказчика в связи с нарушением со стороны Исполнителя прав третьих лиц, связанных с выполняемыми по Договору услугами, относятся на Исполнителя.

13. ПРОЧИЕ УСЛОВИЯ

13.1. С даты заключения настоящего Договора все предыдущие переговоры и переписка по нему теряют силу. Ни одна из Сторон не вправе передавать третьим лицам свои права и обязанности по настоящему Договору без письменного согласия другой Стороны.

13.2. Заказчик вправе в любое время проверить ход и качество оказания услуг Исполнителем.

13.3. Договор составлен в письменной форме.

13.4. Настоящий Договор является действительным при наличии подписей уполномоченных представителей и печатей Сторон.

13.5. Любые изменения и дополнения к настоящему Договору действительны при условии, если они

совершены в письменной форме, подписаны надлежащим образом уполномоченными представителями Сторон и скреплены печатями Сторон.

13.6. Настоящий Договор составлен в двух подлинных экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

13.7. Договор составлен на русском языке.

13.8. Настоящий Договор вступает в силу с даты его подписания и действует до полного исполнения Сторонами своих обязательств по Договору.

13.9. Заказчик имеет право расторгнуть настоящий Договор в одностороннем порядке при условии направления письменного уведомления в адрес Исполнителя не менее чем за 3 дня до предполагаемой даты расторжения.

13.10. По согласованию с Заказчиком Исполнитель вправе осуществить замену соисполнителя из числа СМСП, указанного в плане привлечения соисполнителей из числа СМСП, с которым заключается либо ранее был заключен договор, на другого исполнителя из числа СМСП при условии сохранения цены договора, заключаемого или заключенного между Исполнителем и соисполнителем, либо цены такого договора за вычетом сумм, выплаченных Исполнителем в счет исполненных обязательств, в случае если договор был частично исполнен. В случае замены соисполнителя Стороны Договора подписывают новый план привлечения соисполнителей из числа СМСП в соответствии с формой Приложения № 2 к настоящему Договору без заключения дополнительного соглашения. *(условие исключается в случае заключения Договора с Исполнителем из числа СМСП или в случае отсутствия в ДоЗ требования о привлечении соисполнителей из числа СМСП).*

14. ПРИЛОЖЕНИЯ К ДОГОВОРУ

Приложение № 1 Форма Задания Заказчика.

Приложение № 2 Форма плана привлечения субисполнителей из числа СМСП.

15. АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

Заказчик

Исполнитель

Адрес места нахождения и почтовый адрес:

Адрес места нахождения и почтовый адрес:

т. (____) _____

факс (____) _____

e-mail: _____

ОГРН _____

ИНН _____

КПП _____

Р/счет № _____ в _____

БИК _____

К/счет _____

ОКПО _____

ОКВЭД _____

М.П.

т. (____) _____

факс (____) _____

e-mail: _____

ОГРН _____

ИНН _____

КПП _____

Р/счет № _____ в _____

БИК _____

К/счет _____

ОКПО _____

ОКВЭД _____

М.П.

ЗАДАНИЕ ЗАКАЗЧИКА

Общество с ограниченной ответственностью «БАРНАУЛЬСКИЙ ВОДОКАНАЛ» (ООО «БАРНАУЛЬСКИЙ ВОДОКАНАЛ») в лице Генерального директора Полуго Андрея Сергеевича, действующего на основании Устава, с одной стороны, именуемое в дальнейшем «Заказчик», с одной стороны, и _____ «_____», именуемое в дальнейшем «Исполнитель», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», договорились о предоставлении Исполнителем следующих видов услуг:

№ п/п	Перечень оказываемых Исполнителем услуг g модернизации АСУ ТП	Сроки оказания Исполнителем услуг	Ед. изм.	Количество	Стоимость, руб. без НДС
1	Поставка				
	Право использования программы для ЭВМ SCADA 4D. Клиент-серверная исполнительная система на 30 000 внешних точек ввода. Включает протоколы, 20 счетчиков электроэнергии, 10 счетчиков тепла и энергии	С даты подписания договора до 15.12.2026г.	шт	1	
	Право использования программы для ЭВМ SCADA 4D. Опция резервирования для клиент-серверной исполнительной системы на 30 000 внешних точек ввода-вывода		шт	1	
	Право использования программы для ЭВМ SCADA 4D. Пакет из 10 клиентских рабочих мест с управлением на неограниченное количество точек ввода-вывода		шт	1	
	Право использования программы для ЭВМ SCADA 4D. Клиент-серверная исполнительная система на 10 000 внешних точек ввода, включающие различные протоколы, 20 счетчиков, 10 счетчиков оэнергии и тепла..		шт	1	
	Право использования программы для ЭВМ SCADA 4D. Опция резервирования для клиент-серверной исполнительной системы на 10 000 внешних точек ввода-вывода -1 шт.		шт	1	
	Право использования программы для ЭВМ SCADA 4D. Пакет из 5 клиентских рабочих мест с управлением на неограниченное количество точек ввода-вывода		шт	1	
	Лицензии на программу для ЭВМ		шт	4	
	Лицензия на операционную систему специального назначения для 64-х разрядной платформы на базе процессорной, уровень защищенности "Усиленный" (Воронеж) , способ передачи электронный, серверая до 2-х сокетов		шт	1	
	Лицензия на операционную систему		шт	1	

	специального назначения для 64-х разрядной платформы на базе процессорной, уровень защищенности "Усиленный" (Воронеж), способ передачи электронный, для рабочей станции.				
	ПО Kasperski EDR-для бизнеса Оптимальный		шт	21	
	Средства анализа защищенности "Сканер-ВС". Лицензия на 128 IP адресов		шт	1	
	Средства анализа защищенности "Сканер-ВС". Дополнительный IP к лицензии		шт	14	
2	Поставка и установка АРМ,.	С 17.12.2026г.	шт	7	
	Поставка серверного оборудования.	по 01.03.2027г.	шт	4	
	Поставка щита контроля параметров		шт	1	
	Поставка и установка ультразвуковых датчиков уровня		шт	12	
	Монтаж и ПНР		ед	1	
3	Разработка SCADA ЦДП	С 01.02.2027г.	ед	1	
	Разработка SCADA ОСПВ	по 01.07.2027г.	ед	1	
	Монтаж и ПНР системы ЦДП		ед	1	
	ПНР системы ОСПВ		ед	1	
4	Поставка и установка средств обеспечения ИБ HW 1000	С 01.02.2027г.	компл	3	
	Поставка и установка средств обеспечения ИБ HW 100	по 01.05.2027г.	компл	3	
	Настройка средств ИБ HW 1000		ед	3	
	Настройка средств ИБ HW 1000		ед	3	
5	Настройка сертифицированной ОС на сервере	С 02.07.2027г.	ед	9	
	Настройка сертифицированной ОС на рабочем месте	по 15.12.2027г.	ед	7	
	Установка и настройка антивируса на сервере		ед	9	
	Установка и настройка антивируса на рабочем месте		ед	7	
	Установка и настройка средств защищенности Сканер ВС		ед	1	

Дополнительные условия: Основные требования к оказываемым услугам отражены в Приложении № 1.1 к Заданию заказчика.

Периодичность составления универсального передаточного документа: по готовности согласно перечню оказываемых услуг.

Стоимость объема оказанных услуг по каждому этапу отражена в таблице .

ПОДПИСИ СТОРОН

Заказчик

Адрес места нахождения и почтовый адрес:

т. (____) _____
факс (____) _____
e-mail: _____
ОГРН _____
ИНН _____
КПП _____

Исполнитель

Адрес места нахождения и почтовый адрес:

т. (____) _____
факс (____) _____
e-mail: _____
ОГРН _____
ИНН _____
КПП _____

Р/счет № _____ в

БИК _____

К/счет _____

ОКПО _____

ОКВЭД _____

_____/_____/

М.П.

Р/счет № _____ в

БИК _____

К/счет _____

ОКПО _____

ОКВЭД _____

_____/_____/

М.П.

Технические требования на разработку и поставку системы управления технологическими процессами верхнего уровня ООО «Барнаульский Водоканал»

1. ТРЕБОВАНИЯ К СИСТЕМЕ

1.1 Требования к системе в целом

АСУ ТП должна создаваться на базе унифицированных комплексов технических средств (КТС).

Программное обеспечение должно быть российского производства и включено в реестр Минцифры.

Режим функционирования АСУ ТП – непрерывный с периодическими осмотрами и регламентными работами без останова основного процесса.

АСУ ТП должна быть реализована как распределенная, иерархическая, многофункциональная, программируемая автоматизированная система контроля, управления.

Разрабатываемая система должна соответствовать ГОСТ 24.104-2023 «Автоматизированная система управления. Общие требования», федеральным нормам и правилам в области промышленной безопасности и требованиям, изложенным в настоящих Технических требованиях и иметь возможность дальнейшего развития.

Документация на АСУ ТП должна быть выполнена в соответствии с требованиями комплексов стандартов и руководящих документов на автоматизированные системы (ГОСТ 34.201-2020, ГОСТ Р 59793-2021, ГОСТ 34.602-2020, ГОСТ Р 59853-2021).

Операционная система серверного оборудования должна быть на основе системы Linux, русифицированная и соответствующая требованиям безопасности и производительности.

Необходимо предусмотреть установку сервера реального времени российского производства с поддержкой синхронизации со спутниковыми системами GPS и ГЛОНАСС. Настроить синхронизацию времени оборудования по протоколу NTP от сервера времени.

Срок гарантийного сопровождения оборудования – 3 года после ввода объекта в промышленную эксплуатацию.

1.1.1 Требования к структуре и функционированию системы.

Построение системы будет происходить на основе существующей сети передачи данных.

На каждом крупном объекте дополнительно предусмотреть установку коммутационного сетевого оборудования при необходимости.

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

Взаимодействие двух серверов на объекте должно быть основано на принципе «ведущий-ведомый» с самоподхватом при любой неисправности «ведущего».

Адресное пространство всей сети Ethernet ВУ АСУ ТП должно быть приведено к единому виду.

1.1.2 Требования по сохранности информации при авариях.

Компоновка серверного оборудования должна обеспечивать стабильную работу системы при любых неисправностях и резервирование компонентов сервера от блоков питания до носителей данных. Носители данных должны быть в RAID-массиве уровня, обеспечивающего максимальную защиту от потери данных и возможность горячей замены носителей с функцией восстановления данных на новом носителе после замены.

Каждый из серверов должен иметь свою базу данных с глубиной архивирования тегов 3 года.

Дополнительно устанавливается сервер баз данных для хранения значений тегов с глубиной архивирования 10 лет.

Базы данных серверов должны быть интегрированы в интерфейс пользователя без необходимости дополнительных настроек для получения данных.

Серверное оборудование и оборудование связи должно быть обеспечено ИБП (источник бесперебойного питания).

ИБП должен обеспечить работу оборудования серверов и связи в течении 30 мин при потере основного питания.

1.1.3 Требования к надежности

В составе поставляемого оборудования должны использоваться надежные устройства внешней памяти (жесткие диски) для сохранения и восстановления ретроспективной информации.

Блоки питания должны быть оборудованы защитой от скачков напряжения и токовой отсечкой для сохранения основного оборудования.

Для выявления неисправности компонентов должна быть предусмотрена внешняя световая (звуковая) индикация неисправного состояния. Замена неисправного модуля должна производиться без остановки технологического процесса. Переход на резерв должен производиться автоматически, безударно и без остановки технологического процесса.

Программное обеспечение (ПО) должно быть обеспечено контролем зависания, контролем разрыва связи, инструментами самовосстановления работоспособности.

ПО должно иметь функцию обновления компонентов без прерывания работы системы.

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 часов;
- 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:

- 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;
- реализация постоянного контроля за целостностью хранимой информации;
- организация защиты базы данных и программного обеспечения от несанкционированного вмешательства;
- обеспечение запасными частями.

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.

1.1.4 Требования по обеспечению информационной безопасности.

Для обеспечения штатного режима функционирования АСУ ТП должен быть предусмотрен Исполнителем комплекс организационных и технических мер, составляющих систему защиты информации АСУ ТП и обеспечивающих информационную безопасность в соответствии с требованиями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», приказа ФСТЭК России № 31 от 14.03.2014 г. «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».

Требования по обеспечению информационной безопасности АСУ ТП указаны в Приложении Б.

1.1.5 Требования к эргономике и технической эстетике

Условия работы персонала должны соответствовать ГОСТ 12.3.002-2014.

Взаимодействие персонала с АСУ ТП осуществляется через специализированные АРМ.

Интерфейс разрабатываемой системы АСУ ТП должен быть интуитивно-понятным, позволяющим пользователю в кратчайшие сроки освоить работу с АСУ ТП. 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.

1.1.6 Требования к безопасности к SCADA-системам

1.1.6.1. В целях информационной безопасности и прогнозируемости нагрузки на программно-аппаратный комплекс доступ сторонних пользователей к SCADA должен быть запрещен.

1.1.6.2. Аутентификация (подтверждение подлинности) пользователей должна осуществляться на основе использования имени и пароля, при осуществлении удаленного доступа должна быть использована двухфакторная аутентификация. Аутентификация пользователей должна быть настроена в соответствии с политикой парольной защиты.

1.1.6.3. Доступ пользователей к информационным ресурсам SCADA должен осуществляться согласно функциональной деятельности пользователей, структурных подразделений Заказчика.

1.1.6.4. Доступ к информационным ресурсам SCADA должен осуществляться в соответствии с матрицами доступа по принципу «что не разрешено, то запрещено».

1.1.6.5. Сегменты сети должны быть разделены на сети нижнего и верхнего уровня. Нижний уровень (НУ) должен включать в себя сервера SCADA, ПЛК, преобразователи интерфейсов. Верхний уровень (ВУ) должен включать в себя сервера SCADA, АРМ.

1.1.6.6. Системное и прикладное ПО должно предоставлять возможность смены паролей или блокировки (удаления) учетных записей, в том числе предустановленных и/или используемых для взаимодействия с базами данных.

1.1.6.7. Установка обновлений системного и прикладного программного обеспечения АРМ и серверов SCADA, а также АСО, ПЛК должна производиться в исключительных случаях в ручном режиме во время плановых профилактических мероприятий.

1.1.6.8. Должна быть реализована возможность контроля целостности ПО, включая их обновления, с использованием контрольных сумм, хэш-функции или электронной подписи в процессе загрузки или динамически в процессе работы SCADA систем. Использование автоматизированных средств контроля состава и целостности ПО, при их наличии, не должно каким-либо образом влиять на работу ПО самой SCADA (блокировать или останавливать работу программ, удалять файлы), только регистрировать факт нарушения с указанием названия измененного программного модуля.

1.1.7 Требования к защите от влияния внешних воздействий

Ввиду установки оборудования АСУ ТП в отапливаемых помещениях с обеспечением необходимого микроклимата, особых требований к защите от воздействия от атмосферных помех не предъявляется.

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

АСУ ТП должна сохранять работоспособность при воздействии промышленных радиопомех по нормам 8-72 «Общие нормы допустимых промышленных помех».

1.1.8 Требования к эксплуатации, ТО, ремонту и хранению компонентов системы.

АСУ ТП должна эксплуатироваться в режиме круглосуточной непрерывной работы.

Профилактическое и ремонтное обслуживание отдельных частей АСУ ТП должно проводиться во время остановки на профилактическое и ремонтное обслуживание контролируемого технологического оборудования.

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

Условия хранения ЗИП и аппаратуры АСУ ТП (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 АСУ ТП должны соответствовать требованиям ГОСТ Р 52931-2008.

1.1.9 Требования по стандартизации и унификации.

Аппаратура АСУ ТП 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 АСУ ТП. 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.

1.1.10 Дополнительные требования

Перспективы развития, модернизации системы

Загрузка процессоров и оперативной памяти на АРМ и серверах при полностью загруженном и функционирующем программном обеспечении не должна превышать 50%.

В шкафах распределения питания должен быть предусмотрен резерв в размере 20% по каждому номиналу автоматических выключателей.

Сетевое оборудование должно обеспечивать 50% резервных портов для подключения дополнительного оборудования при необходимости.

Программное обеспечение серверов должно быть снабжено удобными инструментами разработки:

- объектно-ориентированный подход к разработке на всех уровнях проекта;
- обработка данных с помощью встроенного компилируемого языка сценариев;
- гибкая генерация событий на основе поступающих значений по заданным шаблонам;
- сохранение и восстановление среза текущих значений параметров в файл.

Система должна иметь возможность добавления новых клиентов, АРМов, а также систем управления, отдельных контроллеров по протоколам:

- OPC UA;
- OPC DA;
- МЭК-101;
- МЭК-104;
- Modbus TCP;
- Modbus RTU;
- S7.NET;
- SNMP.

Исполнитель должен провести обучение специалистов организации заказчика по:

- проведению ТО оборудования;
- методам выявления неисправностей оборудования;
- созданию резервных копий носителей данных и ПО оборудования;
- добавлению новых объектов к существующей системе;
- редактированию существующих объектов.

Технические средства программируемого логического контроллера АСУ ТП, 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.

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.

Класс защиты шкафов соответствует IP 42. Для шкафов, устанавливаемых в серверных помещениях, допускается использование с классом защиты IP 21.

Мониторы АРМ должны соответствовать требованиям Российских санитарных норм «СП 2.2.3670-20: Санитарно-эпидемиологические требования к условиям труда». Допустимым является применение мониторов, соответствующих стандартам: TC095, TC092, MPRII.

Для защиты обслуживающего персонала и программно-технического комплекса (далее-ПТК) АСУ ТП от возникновения разности потенциалов на контуре заземления в местах установки разнесенного оборудования, вызванного короткими замыканиями в электрической части, атмосферными разрядами, протеканием уравнивающих токов по контуру заземления и т.п. должны предусматриваться заземление компонентов КТС АСУ ТП в соответствии с ПУЭ.

1.2 Требования к функциям (задачам), выполняемым системой

1.2.1 Объем автоматизации

Объем автоматизации определяется в соответствии с количеством входных/выходных технологических параметров, количеством параметров сигнализации, регулирования, управления.

Расчетное количество каналов до 10000.

В процессе наладки системы количество каналов может меняться в пределах 10% от расчетного количества.

1.2.2 Функции системы

АСУ ТП 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 АСУ ТП;
- 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;
- сглаживание и фильтрация сигнала с помехами (при необходимости);
- отказ микропроцессорных контроллеров;
- обрыв одного из проводов резервируемой сети;
- отказ рабочих станций, как оборудования, так и программного обеспечения.

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;
- представление одиночных и групповых трендов параметров с заданной продолжительностью предыстории;
- 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 РСУ.

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 36 месяцев;
- архивация значений параметров с дискретностью не более 30 секунд, срок хранения на серверах баз данных в течении 10 лет;

- формирование журнала событий для регистрации действий операторов, включения выключения технологического оборудования;
- формирование текущих, сменных, суточных, месячных, хозрасчетных рапортов по заданной форме;
- формирование отчетов о нарушении режима;
- хранение базы данных контроллеров подсистем управления;
- 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 АСУ ТП.
- для всех позиций (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).

1.3 Требования к видам обеспечения

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.

1.3.1 Требования к техническому обеспечению

Шкафы с оборудованием серверов АСУ ТП должны соответствовать следующим требованиям:

- двухсторонний доступ (с цоколем, без дверей, замков) 800Шx2100Вx800Г;
- 40-42U;
- с верхним подводом кабелей;
- иметь встроенное внутреннее освещение и розетку 220В;
- иметь однорядные клеммники с ножевыми размыкателями или предохранительными вставками;
- с шиной центрального заземления;
- в шкафах системы управления предусмотреть размещение оптических кросс-боксов и сетевого оборудования;
- в каждом серверном шкафу установить сетевое оборудование достаточное для полноценного функционирования системы;
- клеммные терминалы для подключения полевых кабелей и кабелей межшкафного соединения;
- клеммные терминалы для подключения полевых кабелей должны быть с ножевыми размыкателями с винтовыми зажимами;
- пластиковые кабель-каналы с учетом разделения кабелей по типу сигнала;
- установить систему мониторинга климата оборудования шкафов и серверной (пример: модуль мониторинга VT825). Модуль должен передавать данные в систему SCADA по климату внутри шкафа и внутри помещения серверной, также данные с дискретных датчиков открытия дверей серверной.

Требования к составу и оборудованию АРМов указаны в Приложении В.

К дополнительным АРМам (режим просмотра) относятся:

1. АРМ Директора по производству;
2. АРМ Главного метролога АСУТП;
3. АРМ Начальника участка по ремонту и обслуживанию КИПиА;
4. АРМ Инженера по метрологии;

5. АРМ Начальника цеха ОСПВ;
6. АРМ Инженера-технолога ОСПВ;
7. АРМ Начальника технического отдела.

Компоновка оборудования АРМов должна удовлетворять потребностям развернутого на них программного обеспечения.

Для всех системных блоков всех типов АРМ и Серверов (при их наличии) предусмотреть резервирование жестких дисков (HDD) в конфигурации RAID.

АРМ операторов-технологов и инженерные станции должны быть оснащены звуковыми колонками, кронштейн для крепления и установки на рабочем месте соответствующего количества мониторов.

Все АРМ должны быть равнозначны по набору функций контроля и управления.

Инженерная станция должна совмещать инженерный и операторский функционал с разделением полномочий, защищенных паролем.

АРМы должны иметь возможность разграничения прав доступа на различных уровнях взаимодействия с системой.

На дополнительных АРМах взаимодействие с системой должно быть ограничено только просмотром состояния системы без элементов управления.

АРМ должен иметь средства для сохранения конфигурации системы на сменные носители.

Требования к интерфейсу оператора указаны в Приложении А.

1.3.2 Требования к программному обеспечению.

Программное обеспечение должно удовлетворять следующим требованиям:

- программное обеспечение должно быть Российской разработки и включено в реестр Минцифры;
- 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 ПТК системы в соответствии с условиями производственных задач;
- надежность (живучесть) ПО - способность выполнять возложенные на систему функции в соответствии с заданным алгоритмом при действии дестабилизирующих факторов (сбои и отказы оборудования, несанкционированный доступ в программу и т.п.).

Программное обеспечение должно включать антивирусное ПО, протестированное на совместимость с ПО АСУ ТП.

В состав ПО должны входить общесистемное ПО (СПО), базовое прикладное ПО (БПО) и собственно прикладное ПО (ППО) с соответствующими структурами данных.

В качестве общесистемного ПО должны использоваться современные стандартные универсальные и однотипные операционные системы, поддерживающие сетевые функции.

Общесистемное ПО (универсальные ОС) должны надежно функционировать в многозадачном режиме и обеспечивать функционирование прикладного ПО в реальном масштабе времени с защитой от сбоев. В состав системного программного обеспечения должны входить программные средства создания и ведения баз данных, их структурные описания, описания взаимосвязей баз данных.

Базовое прикладное ПО должно включать в себя развитые инструментальные и исполнительные средства (пакеты программ) производителей оборудования АСУ ТП, позволяющие эффективно разрабатывать, отлаживать и исполнять компоненты прикладного ПО АРМ и баз данных системы.

Прикладное ПО АСУ ТП на всех уровнях системы должно функционировать под управлением соответствующих ОС и БПО и должно включать следующие компоненты:

- оперативное ПО (оперативное ПО АРМ, ОС)
- тестовые программы и программы диагностики технических средств системы;
- программы и средства работы с БД АСУ ТП;

- ПО для создания проектов, конфигурирования системы на инженерной станции;
- ПО для создания мнемосхем (видеоэкранов) на инженерной станции;
- ПО для автоматического документирования базы данных и алгоритмов системы;
- ПО для формирования рапортов, отчетов;
- ПО для анализа сигнализаций и сообщений (система управления сигнализациями).

1.3.2.1 Требования к SCADA-системам

SCADA - система сбора данных и оперативного контроля, предназначенная для получения и хранения информации о текущем режиме системы и состоянии оборудования от системы сбора и передачи информации, обработки полученной информации и предоставления информации подсистемам автоматизированной системы диспетчерского управления и другим автоматизированным системам (далее-SCADA), должна соответствовать требованиям Технической политики Компании «РОСВОДОКАНАЛ» и настоящих технических требований, которые должны учитываться при разработке проектной документации на ее создание или модификацию;

- SCADA должна быть Российской разработки и включена в реестр Минцифры.
- архитектура SCADA должна соответствовать принципам открытости архитектуры и должна быть построена на основе общедоступных и общепризнанных стандартов на продукты информационных технологий. Для успешного решения поставленных задач SCADA должна обеспечивать:
 - масштабируемость;
 - возможность интеграции и обмена информацией с внешними программно-аппаратными комплексами;
 - информационную унификацию путем применения общей информационной модели;
 - наличие необходимой и достоверной информации для задач оперативно-диспетчерского управления. Необходимая информация поступает извне (является внешней по отношению к SCADA) или вырабатывается в процессе управления (внутри SCADA);
 - защиту от несанкционированного доступа к информации и функциям SCADA;
 - защиту от ошибочных действий персонала, от случайных изменений и разрушения информации и программ.
- Аппаратные и программные средства должны иметь модульную структуру и системное ПО, допускающие широкий диапазон их использования от минимального выбора для выполнения одной функции до максимального, обеспечивающего выполнение всех функций SCADA.
- SCADA должна отвечать следующим требованиям к программному продукту:
 - полная кроссплатформенность среды разработки и среды исполнения;
 - поддержка наиболее распространенных отечественных операционных систем;
 - поддержка наиболее распространенных отечественных процессоров;
 - поддержка широкого набора промышленных протоколов, в том числе проприетарных (Ethernet/IP, Profinet, EtherCAT, FINS, SLMP, SNMP и др.);
 - вывод на мнемосхему видеопотока в формате RTSP;
 - поддержка протокола OPC UA в режимах сервера и клиента, с передачей архивных данных, поддержкой Reverse Connection, различных режимов шифрования и подписи, а также режима OPC Alarms and Events (тревоги и события);
 - прямая поддержка электро- и теплосчетчиков (Меркурий, Энергомера, Пульсар, Теплоком и др.);
 - наличие заключения о возможности применения на значимых объектах критической информационной инфраструктуры не ниже 1 категории значимости в соответствии с приказом ФСТЭК России от 25.12.2017 № 239.
- Среда разработки SCADA должна обеспечивать:
 - поддержку языков программирования по МЭК 61131-3;
 - поддержку языка C# и возможность применения готовых библиотек C#;
 - создание функциональных блоков на языке C++;
 - применение объектно-ориентированного подхода при разработке проекта;

- табличное представление проекта с возможностью дальнейшей обработки внешними инструментами (в том числе Python, Visual Basic, JavaScript и др.);
- наличие готовых специализированных функциональных блоков (расчёт сопротивлений, ПИ- и ПИД-регуляторы, генераторы импульсов и сигналов с настраиваемыми параметрами и выходами и т. п.);
- неограниченное тиражирование предварительно созданных элементов (объектов) как со строгим наследованием настроек, так и с возможностью изменения отдельных настроек пользователем;
- наличие библиотеки стандартных анимируемых элементов;
- добавление и анимацию пользовательских SVG-элементов;
- интеграцию с внешними системами по API;
- работу с внешними базами данных (PostgreSQL, MS SQL, АВАДС, MySQL, ClickHouse);
- интеграцию с информационными моделями зданий и сооружений (BIM);
- отображение и привязку к проекту цифрового двойника технологического объекта;
- совместимость с конфигураторами систем диспетчеризации инженерного оборудования зданий.
- SCADA должна обеспечивать выполнение следующих требований по информационной безопасности:
 - наличие функционала, позволяющего в максимальной степени выполнить требования действующих стандартов по информационной безопасности;
 - аутентификацию посредством службы каталогов Active Directory (LDAP, с перспективой перехода на LDAPS для операционных систем на базе Linux);
 - ролевую модель и разделение прав доступа к информации;
 - наличие отдельного интерфейса для добавления пользователей и ролей, а также для управления пользовательскими и ролевыми настройками;
 - наличие набора функциональных блоков для добавления пользователей и ролей и управления их настройками внутри проекта;
 - шифрование по протоколу не ниже TLS 1.3 при удалённом подключении клиентов визуализации (браузер или специализированное приложение) к web-серверу;
 - хранение пользовательских настроек в отдельной базе данных, доступной для нескольких проектов, при этом пароль должен быть зашифрован по алгоритму не слабее argon2 с обязательным применением «соли»;
 - отправку журнала действий оператора на syslog-сервер;
 - ограничение доступа к журналу регистрации событий безопасности;
 - настройку периода хранения и размера журнала регистрации;
 - генерацию уведомлений о переполнении журнала регистрации;
 - контроль целостности программного обеспечения и прикладного программного обеспечения проекта (ППО) — как в автоматическом режиме, так и по команде оператора.

В стоимость программных средств АСУ ТП должна входить стоимость лицензий на используемые программные средства

1.3.2 Требования к лингвистическому обеспечению

- Лингвистическое обеспечение SCADA должно быть достаточным для общения различных категорий пользователей в удобной для них форме со средствами автоматизации SCADA.

В лингвистическом обеспечении SCADA должны быть:

- предусмотрены языковые средства для описания любой используемой информации в SCADA;
- стандартизированы описания однотипных элементов информации и записи синтаксических конструкций;
- обеспечены удобство, однозначность и устойчивость общения пользователей со средствами автоматизации SCADA.
- Лингвистическое обеспечение SCADA должно быть отражено в документации (инструкциях, описаниях) организационного обеспечения SCADA в виде правил общения пользователей с программно-техническими средствами во всех режимах функционирования SCADA.

- Интерфейс SCADA, обеспечивающий взаимодействие пользователей с SCADA, должен быть реализован на русском языке.

В средствах (подсистеме) исполнения все выдаваемые на экраны интерфейса оператора текстовые фрагменты: (элементы меню, сообщения, подсказки, элементы протоколов событий и пр.) должны быть на русском языке. Среда программирования КТС должна входить в состав ПТК и обеспечивается Исполнителем.

1.3.4 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 АСУ ТП, 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;
- формы выходных документов;
- технические и программные средства архивирования, записи, хранения и воспроизведения информации;
- технические и программные средства передачи информации между компонентами АСУ ТП и в смежные информационные системы.

Применяемые в выходных документах и на устройствах отображения информации термины и сокращения должны быть общепринятыми в отрасли. Символы, используемые для фрагментов мнемосхемы на экране дисплея, их цветовое кодирование должны быть идентичными.

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

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

Для удобства хранения, обработки и обмена информацией в рамках распределенной системы управления автоматически должна создаваться единая база данных, обеспечивающая доступ к данным с локальных элементов сети, которыми являются:

- многофункциональные операторские станции – рабочие места технологического персонала;
- инженерные станции – рабочие места инженеров АСУ ТП.

Обслуживание базы данных АСУ ТП должно выполняться только с инженерной станции в режиме санкционированного доступа.

Информационная совместимость АСУ ТП и смежных систем обеспечивается применением стандартных протоколов обмена данными:

- Ethernet/IP;
- Modbus (TCP, RTU).

1.3.4.1. SCADA для обеспечения технологических процессов управления необходима информация о технологических режимах работы объектов диспетчеризации.

1.3.4.2. В состав информации о технологическом режиме работы объекта диспетчеризации входят:

- электрические параметры режима, включая параметры аварийных режимов, характеризующие технологические режимы объектов;
- неэлектрические параметры, отражающие условия работы объектов;
- команды дистанционного управления и регулирования.

413.4.3. SCADA должна обеспечивать прием и обработку всего необходимого объема параметров, характеризующих технологические режимы объектов.

1.3.4.4. Перечень (детальный состав) параметров и команд управления определяется требованиями:

- обеспечения наблюдаемости и управляемости режима работы объекта;

- обеспечения надежности и достоверности информации о технологических режимах объектов за счет ее избыточности;
- регламентирующих документов по режимной и противоаварийной автоматике.

1.4. Требования к обмену информацией с системой сбора и передачи информации.

- SCADA должна обеспечивать сохранение меток единого астрономического времени для всех принимаемых параметров. Для меток времени должно использоваться UTC.

Форматы данных, используемые для передачи информации о телесигналах, телеизмерениях, специальных параметрах должны обеспечивать передачу:

- текущего значения параметра;
- признаков достоверности (описателя качества) параметра;
- метки времени параметра (при передаче по изменению).

Значения телеметрической информации (ТИ) должны передаваться в инженерных единицах. Непосредственная передача результатов аналого-цифрового преобразования (квантов) допускается в исключительных случаях по согласованию с Заказчиком.

2. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ АСУ ТП

Разработка АСУ ТП осуществляется в соответствии с ГОСТ Р 59793-2021 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» и ввод в действие АСУ ТП осуществляется в соответствии с требованиями СП 77.13330-2016 «Системы автоматизации».

Разработчик АСУ ТП осуществляет поставку оборудования, выполнение техно рабочего проекта, шеф-монтажных (ШМР), пуско-наладочных (ПНР) и инжиниринговых работ – далее Поставщик.

2.2 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 и Генеральным Проектировщиком/Проектировщиком (дается не полный перечень):

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

В состав окончательной документации входят (перечень не исчерпывающий):

- комплектная документация системы;
- 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;
- инструкция по заземлению.

Содержание окончательной документации должно быть согласовано Заказчиком.

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

Документация предоставляется в электронном виде и на бумажном носителе в 1 экз.

2.3 Проверка и испытания АСУ ТП

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 АСУ ТП состоит из нескольких этапов (см. ГОСТ Р 59793-2021, СП77.13330-2016 «Системы автоматизации»):

- 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 или оборудования инженерных систем, 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;
- III стадия - комплексная наладка систем автоматизации.

На этапе «Предварительные испытания» осуществляют:

- испытания программно-технического комплекса в соответствии с программой и методикой предварительных испытаний; устранение неисправностей и внесение изменений в документацию АС ТП, 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 АСУ ТП 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 магнитных 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.

Приложения:

1. Приложение А – Требования к интерфейсу оператора
2. Приложение Б – Требования ИБ к АСУ ТП

ТРЕБОВАНИЯ К ИНТЕРФЕЙСУ ОПЕРАТОРА

A.1 Требования к размещению и компоновке рабочих мест

A.1.1 Система должна включать автоматизированные рабочие места:

- операторов;

A.1.2 Рабочие места должны быть укомплектованы:

- АРМ Оператора – двумя жидкокристаллическими мониторами;

A.1.3 Управление технологическим процессом должно производиться с помощью манипулятора «мышь» и универсальной алфавитно-цифровой клавиатуры (рус./лат.).

A.2 Общие требования

A.2.1 Основным средством представления информации оператору должен являться цветной графический монитор.

A.2.2 Технологические сообщения оператору должны быть на русском языке, системные сообщения могут быть на английском и русском языках.

A.2.3 Для операторского интерфейса должна быть предусмотрена система защиты от несанкционированного доступа к изменяемым параметрам Системы.

A.3 Структура операторского интерфейса

A.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.

A.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;

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

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

A.3.4 Операторский интерфейс должен включать стандартные видеограммы:

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

A.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.

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

A.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.

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

A.4 Отображение информации на мнемосхемах

A.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.

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

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

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

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

Цвет и способ сигнализации настраиваются при конфигурировании.

A.4.5 Цветовое кодирование состояния запорной арматуры.

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

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

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

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

A.5 Сигнализация

A.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;
- аварийный останов технологического оборудования (насосы, компрессоры, вентиляторы);
- отказ оборудования Системы;
- отключение внешнего электропитания и переход на резервное электропитание.

A.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;

Текстовое оповещение о событиях (технологическая сигнализация, системное сообщение и т.п.) должно отображаться в специальной строке графического интерфейса распределительной системы управления (далее - РСУ).

A.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.

A.5.4 При срабатывании аварийно-предупредительной сигнализации должна быть предусмотрена возможность вызова на экран (с помощью манипулятора «мышь») соответствующей мнемосхемы технологического процесса.

A.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 силового оборудования за месяц, за заданный период, вызывается на печать по требованию персонала;

- Отчет о переключениях механизмов за сутки, за месяц, за заданный период;

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

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУТП

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система управления технологическим процессом (АСУ ТП) — комплекс программных и технических средств, предназначенных для контроля и управления технологическим оборудованием и связанными с ним процессами.

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Персональная учетная запись — уникальный идентификатор, закрепленный за конкретным физическим лицом, исключающий коллективное использование одних и тех же реквизитов доступа.

Программируемый логический контроллер (ПЛК) — микропроцессорное устройство, предназначенное для сбора данных, логической обработки и управления исполнительными механизмами на технологическом уровне.

Межсетевой экран (МЭ) — средство защиты, осуществляющее контроль и фильтрацию сетевого трафика в соответствии с заданными правилами безопасности.

Целостность информации — состояние информации, при котором отсутствует любое ее несанкционированное изменение.

Доступность информации — состояние информации, при котором субъекты, имеющие права доступа, могут беспрепятственно получать и использовать её.

Контролируемая зона — пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих допуска.

Нештатная ситуация — отклонение в работе АСУ ТП от нормального режима, вызванное техническим сбоем, ошибкой персонала или внешним воздействием.

Регламент (инструкция) — организационный документ, устанавливающий обязательный порядок выполнения действий по обеспечению безопасности и эксплуатации системы.

2. СОКРАЩЕНИЯ

АВЗ — антивирусная защита;

АРМ — автоматизированное рабочее место;

АСО — Активное сетевое оборудование;

АСУ ТП — автоматизированная система управления технологическим процессом;

АУД — аудит безопасности;

БД — база данных;

ДНС — обеспечение действий в нештатных ситуациях;

ЗНИ — защита машинных носителей информации;

ЗИС — защита сетевого взаимодействия;

ЗТС — защита технических средств и систем;

ИАФ — идентификация и аутентификация;

ИНЦ — реагирование на компьютерные инциденты;

МЭ — межсетевой экран;

ОДТ — обеспечение доступности;

ОПО — управление обновлениями программного обеспечения;

ОС — операционная система;

ОЦЛ — обеспечение целостности;

ПЛК — программируемый логический контроллер;

ПЛН — планирование мероприятий по обеспечению защиты информации;

ПО — программное обеспечение;

СПО — системное программное обеспечение;

ТЗ — техническое задание;

УКФ — управление конфигурацией;

УПД — управление доступом;

ФСТЭК России — Федеральная служба по техническому и экспортному контролю;

DMZ — демилитаризованная зона;

UTM — универсальный шлюз безопасности;

VPN — виртуальная частная сеть.

3. ОБЩИЕ ПОЛОЖЕНИЯ

Защита информации в АСУ ТП является составной частью работ по созданию (модернизации) и эксплуатации системы и обеспечивается на всех стадиях ее жизненного цикла. Принимаемые организационные и технические меры защиты информации:

- должны обеспечивать доступность и целостность обрабатываемой информации, а также ее конфиденциальность (в случаях, установленных проектной документацией);

- должны быть интегрированы с мерами по промышленной, физической и пожарной безопасности и не должны препятствовать выполнению требований по обеспечению безопасности технологического процесса;

- не должны оказывать отрицательного влияния на штатный режим функционирования, надежность и отказоустойчивость АСУ ТП.

Требования к обеспечению защиты информации определяются в соответствии со следующими нормативными документами:

- Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

4. ТРЕБОВАНИЯ К МЕРАМ ЗАЩИТЫ ИНФОРМАЦИИ В АСУ ТП

Настоящие требования предъявляются к комплексу программно-технических средств всех уровней АСУ ТП, а также к организационному обеспечению процессов эксплуатации системы. Набор мер защиты информации для АСУ ТП с учётом присвоенного класса защищённости «3» включает:

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА

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

Должен быть реализован комплекс мер, обеспечивающий строгое разграничение доступа к компонентам АСУ ТП за счет:

1. Документальное оформление (ИАФ.0): Разработка регламента (политики), определяющего правила назначения прав, требования к сложности паролей и порядок действий при компрометации учетных записей.
2. Идентификация и аутентификация пользователей, управление их идентификаторами и средствами аутентификации (ИАФ.1, ИАФ.3, ИАФ.4): Обеспечения реализации создания персональных учётных записей для каждого пользователя и процесса с использованием отечественного сертифицированного программного обеспечения (в том числе служб каталогов и систем управления доступом, включенных в реестр российского ПО) или сертифицированных встроенных механизмов защиты СПО. Использование общих (групповых) учётных записей не допускается. Механизмы должны поддерживать блокировку при переборе паролей и контроль срока их действия.
3. Контроля оборудования (ИАФ.2): Технического ограничения возможности подключения к сети АСУ ТП сторонних устройств (привязка по MAC-адресам, использование сертификатов или блокировка неиспользуемых портов).
4. Безопасного внешнего доступа (ИАФ.5): Обеспечения однозначной идентификации внешних пользователей и ограничения удаленного доступа к компонентам АСУ ТП только для авторизованных лиц.

5. Криптографической защиты (ИАФ.7): Использования защищенных протоколов передачи данных, исключающих передачу аутентификационной информации в открытом виде внутри промышленного сегмента и за его пределами.

Примечание: должна быть реализована возможность изменения паролей, создаваемых по умолчанию, в том числе к системным учетным записям.

УПРАВЛЕНИЕ ДОСТУПОМ

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

Должен быть реализован комплекс мер, для системы управления доступом, исключающих несанкционированные действия пользователей и внешних систем в контуре АСУ ТП:

1. Документальное оформление (УПД.0): Разработка политики управления доступом, определяющей роли, права и обязанности персонала, а также процедуры пересмотра прав доступа.
2. Управление полномочиями и ролями (УПД.1, УПД.2, УПД.4, УПД.5): Использование отечественного сертифицированного ПО (служб каталогов, систем управления доступом) для создания учетных записей (УПД.1) и реализации ролевой модели доступа. Права должны назначаться исходя из принципа «минимально необходимых привилегий» (УПД.5) для каждой роли (УПД.4), обеспечивая физическое и логическое разграничение доступа к ресурсам (УПД.2).
3. Контроль сеансов и попыток доступа (УПД.6, УПД.10, УПД.11): Настройки механизмов блокировки доступа при превышении заданного числа неуспешных попыток входа (УПД.6), автоматического блокирования сеанса при неактивности пользователя (УПД.10) и жесткого ограничения перечня разрешенных действий в системе до момента успешного прохождения аутентификации (УПД.11).
4. Безопасное взаимодействие (УПД.13, УПД.14): Применения межсетевых экранов и криптографических шлюзов на базе отечественного сертифицированного ПО для реализации защищенного удаленного доступа (УПД.13), а также механизмов фильтрации и контроля трафика при взаимодействии с внешними информационными системами (УПД.14).

Примечание: должен быть реализован регламент управления доступом и актуальная матрица доступа, описывающая права каждой роли (администратор, инженер, оператор) ко всем компонентам АСУ ТП

ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

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

В проекте должны быть предусмотрены технические средства и организационные процедуры, обеспечивающие защиту информации на съемных носителях и контроль интерфейсов ввода-вывода.

Указанные меры реализуются путем применения:

1. Разработка политики защиты машинных носителей информации (ЗНИ.0): создание регламента, определяющего зоны ответственности, правила использования носителей в АСУ ТП и порядок действий персонала.
2. Учет машинных носителей информации (ЗНИ.1): разработка форм реестров (журналов) и порядка присвоения уникальных идентификаторов (маркировки) для обеспечения прослеживаемости носителей.
3. Управление физическим доступом к машинным носителям информации (ЗНИ.2): определение требований к местам безопасного хранения (сейфам, шкафам) и разработка процедур контроля доступа к ним в нерабочее время.
4. Контроль использования интерфейсов ввода (вывода) и подключения машинных носителей информации (ЗНИ.5, ЗНИ.7): внедрение и настройка отечественного сертифицированного ПО для программного управления портами, а также физическое

ограничение (блокировка) доступа к неиспользуемым интерфейсам на уровне аппаратного обеспечения (BIOS/UEFI, опломбирование портов или установка механических блокираторов).

5. Уничтожение (стирание) информации на машинных носителях информации (ЗНИ.8): поставка и настройка отечественного сертифицированного ПО для гарантированного удаления данных, а также разработка инструкции по выводу носителей из эксплуатации.

Примечание: должны быть реализованы утвержденные формы журналов учета машинных носителей, инструкции по маркировке носителей и регламент гарантированного уничтожения информации».

АУДИТ БЕЗОПАСНОСТИ

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

В проекте должны быть предусмотрены инструменты и процедуры непрерывного контроля состояния защиты, регистрации событий и оперативного реагирования на инциденты в АСУ ТП.

Указанные меры реализуются путем применения:

1. Разработка политики аудита безопасности и проведение внутренних аудитов (АУД.0, АУД.10): разработка регламентов, определяющих перечень регистрируемых событий, периодичность их анализа, а также порядок проведения плановых внутренних проверок состояния защищенности системы.
2. Инвентаризация информационных ресурсов (АУД.1): создание и настройка автоматизированных механизмов учета всех компонентов АСУ ТП (ПЛК, АРМ, серверы, сетевое оборудование) с фиксацией их характеристик и мест установки.
3. Анализ уязвимостей и их устранение (АУД.2): использование отечественного сертифицированного ПО для поиска уязвимостей в программном обеспечении и конфигурациях оборудования, а также разработка регламента по их устранению и установке обновлений безопасности.
4. Реагирование на сбои при регистрации событий безопасности (АУД.8): настройка механизмов оповещения администраторов в случае невозможности записи логов (например, при переполнении памяти или отказе хранилища).

Примечание: так же должны быть реализованы формы с перечнем контролируемых событий безопасности, инструкции по анализу журналов и регламент проведения инвентаризации активов.

АНТИВИРУСНАЯ ЗАЩИТА

(АВЗ.0, АВЗ.1, АВЗ.2, АВЗ.4)

В проекте должны быть предусмотрены эшелонированная система антивирусной защиты, обеспечивающая обнаружение и блокирование вредоносного программного кода в контуре АСУ ТП без нарушения работоспособности технологических процессов.

Указанные меры реализуются путем применения:

1. Разработка политики антивирусной защиты (АВЗ.0): создание регламента, определяющего порядок развертывания средств антивирусной защиты, перечень защищаемых объектов, настройки сканирования, а также действия персонала при обнаружении вредоносного ПО.
2. Реализация антивирусной защиты (АВЗ.1): внедрение и настройка отечественного сертифицированного ПО (антивирусных средств), совместимого с используемым в АСУ ТП системным и прикладным программным обеспечением.
3. Антивирусная защита электронной почты и иных сервисов (АВЗ.2): обеспечение фильтрации входящих потоков данных на уровне межсетевых экранов или специализированных шлюзов безопасности с использованием отечественного сертифицированного ПО.
4. Обновление базы данных признаков вредоносных компьютерных программ (АВЗ.4): проектирование и настройка инфраструктуры для безопасного обновления

антивирусных баз внутри изолированного сегмента АСУ ТП, а также разработка инструкции по их регулярной актуализации без прямого доступа в сеть «Интернет».

Примечание: в состав эксплуатационной документации должны входить инструкции по администрированию средств антивирусной защиты, регламент обновления сигнатурных баз в изолированном контуре и протоколы тестирования совместимости антивирусного ПО со специфическим ПО АСУ ТП.

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ

(ОЦЛ.0, ОЦЛ.1)

В проекте должны быть предусмотрены механизмы контроля неизменности программной среды и данных, а также защиты системы от несанкционированных исправлений или повреждений кода.

Указанные меры реализуются путем применения:

1. Разработка политики обеспечения целостности (ОЦЛ.0): создание регламента, определяющего объекты контроля целостности (файлы ОС, прикладное ПО АСУ ТП, конфигурации оборудования), правила проведения проверок и порядок действий персонала при обнаружении нарушений целостности.
2. Контроль целостности программного обеспечения (ОЦЛ.1): внедрение и настройка отечественного сертифицированного ПО, обеспечивающего автоматический контроль целостности исполняемых модулей, системных библиотек и конфигурационных файлов. Механизмы защиты должны обеспечивать блокировку запуска или уведомление администратора при выявлении несанкционированных изменений.

Примечание: в состав эксплуатационной документации должны входить инструкции по настройке средств контроля целостности, перечень контролируемых объектов с указанием их эталонных контрольных сумм, а также регламент периодической проверки целостности ПО АСУ ТП.

ОБЕСПЕЧЕНИЕ ДОСТУПНОСТИ

(ОДТ.0, ОДТ.4, ОДТ.5, ОДТ.6, ОДТ.8)

В проекте должны быть предусмотрены комплекс мер по обеспечению устойчивого функционирования АСУ ТП и возможности оперативного восстановления работоспособности системы после сбоев или инцидентов.

Указанные меры реализуются путем применения:

1. Разработка политики обеспечения доступности (ОДТ.0): создание регламента, определяющего критичные компоненты системы, допустимое время восстановления, а также порядок действий персонала при возникновении нештатных ситуаций и отказов оборудования.
2. Резервное копирование информации, обеспечение возможности восстановления информации и программного обеспечения (ОДТ.4, ОДТ.5, ОДТ.6): внедрение и настройка отечественного сертифицированного ПО для автоматизированного резервного копирования данных и образов операционных систем. Подрядчик обязан спроектировать защищенное хранилище резервных копий и провести тестирование процедур восстановления для подтверждения их работоспособности.
3. Контроль предоставляемых вычислительных ресурсов и каналов связи (ОДТ.8): использование встроенных механизмов мониторинга ОС и активного сетевого оборудования, а также отечественного сертифицированного ПО для контроля загрузки процессоров, оперативной памяти, дискового пространства и пропускной способности каналов связи с целью предупреждения отказов системы из-за нехватки ресурсов.

Примечание: в состав эксплуатационной документации должны входить регламент резервного копирования, инструкции по пошаговому восстановлению программного обеспечения и

данных из резервных копий, а также протоколы успешно проведенного тестового восстановления системы

ЗАЩИТА ТЕХНИЧЕСКИХ СРЕДСТВ И СИСТЕМ

(ЗТС.0, ЗТС.2, ЗТС.3, ЗТС.4, ЗТС.5)

В проекте должны быть предусмотрены комплекс мер по физической защите оборудования АСУ ТП, исключающий несанкционированный доступ к аппаратным средствам и защищающий их от внешних деструктивных воздействий.

Указанные меры реализуются путем применения:

1. Разработка политики защиты технических средств и систем (ЗТС.0): создание регламента, определяющего требования к размещению оборудования, правила доступа в помещения с техническими средствами АСУ ТП и порядок контроля целостности корпусов и шкафов управления.
2. Организация контролируемой зоны и управление физическим доступом (ЗТС.2, ЗТС.3): проектирование границ контролируемой зоны и внедрение технических средств (электронных замков, считывателей, датчиков вскрытия), интегрированных с отечественным сертифицированным ПО систем контроля и управления доступом (СКУД) для регистрации и ограничения входа в пультовые, серверные и к шкафам ПЛК.
3. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4): проектирование расположения мониторов АРМ операторов и крупнопанельных дисплеев таким образом, чтобы исключить возможность визуального съема информации посторонними лицами через окна или дверные проемы.
4. Защита от внешних воздействий (ЗТС.5): использование специализированных защищенных шкафов (класса IP), систем бесперебойного питания, заземления и климат-контроля для защиты технических средств от пыли, влаги, перепадов температуры и электромагнитных помех в соответствии с условиями эксплуатации на объекте.

Примечание: в состав эксплуатационной документации должны входить схемы размещения оборудования с указанием границ контролируемой зоны, инструкции по управлению физическим доступом и регламент проверки целостности печатей (пломб) на аппаратных средствах

ЗАЩИТА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ И ЕЕ КОМПОНЕНТОВ

(ЗИС.1, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.21, ЗИС.32, ЗИС.34, ЗИС.38, ЗИС.39,)

В проекте должна быть реализована сетевая архитектура, обеспечивающая безопасное взаимодействие компонентов АСУ ТП и защита от внешних сетевых атак.

Указанные меры реализуются за счёт:

1. Разработка политики защиты информационной (автоматизированной) системы и ее компонентов (ЗИС.0): создание регламента, определяющего правила сетевого обмена, топологию сети и порядок внесения изменений в сетевую конфигурацию.
2. Защита периметра, эшелонированная защита и организация демилитаризованной зоны (ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.34): внедрение и настройка отечественного сертифицированного ПО и аппаратных средств (межсетевых экранов уровня UTM) для сегментации сети, фильтрации трафика и защиты от атак типа «DoS/DDoS». Для обмена данными с внешними сетями должна быть спроектирована демилитаризованная зона (DMZ).
3. Разделение функций по управлению с иными функциями (ЗИС.1): выделение трафика администрирования в отдельный защищенный сегмент (VLAN) с запретом доступа к нему из технологической сети.
4. Скрытие архитектуры, конфигурации и обеспечение доверенных каналов (ЗИС.8, ЗИС.19,

ЗИС.20): использование механизмов маскировки внутренней структуры сети и применение отечественного сертифицированного ПО (VPN-шлюзов) для шифрования данных при их передаче по открытым каналам связи, обеспечивая создание доверенных маршрутов обмена информацией.

5. Запрет несанкционированной удаленной активации устройств и защита беспроводных соединений (ЗИС.21, ЗИС.32): программное и аппаратное отключение функций удаленного включения периферийных устройств (камер, микрофонов), а также обязательное использование механизмов авторизации и шифрования для разрешенных беспроводных сегментов.
6. Защита информации при использовании мобильных устройств и управление перемещением виртуальных машин (ЗИС.38, ЗИС.39): применение отечественного сертифицированного ПО для контроля мобильных средств доступа (если предусмотрено проектом) и обеспечения безопасности миграции виртуальных ресурсов внутри серверного кластера.

Примечание: в состав эксплуатационной документации должны входить детальная схема сетевой архитектуры, таблицы маршрутизации, перечень разрешенных сетевых протоколов и портов (матрица сетевых доступов), а также инструкции по настройке межсетевых экранов и VPN-шлюзов

РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

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

В проекте должны быть реализованы организационные процедуры и технические инструменты, обеспечивающие своевременное обнаружение, локализацию и ликвидацию последствий компьютерных атак и сбоев в АСУ ТП.

Указанные меры реализуются за счёт:

1. Разработка политики реагирования на компьютерные инциденты (ИНЦ.0): создание регламента, определяющего критерии отнесения событий к инцидентам, состав аварийной команды (группы реагирования), порядок связи и распределение ответственности.
2. Устранение последствий компьютерных инцидентов и принятие мер по предотвращению их повторного возникновения (ИНЦ.4, ИНЦ.5): разработка планов действий по восстановлению работоспособности системы (планов аварийного восстановления) и процедур «разбора полетов» для корректировки настроек средств защиты после инцидента.

Примечание: в состав эксплуатационной документации должны входить регламент реагирования на компьютерные инциденты, пошаговые инструкции для персонала при обнаружении типовых атак и формы отчетов (актов) о результатах расследования инцидентов.

УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ

(УКФ.0, УКФ.2, УКФ.3):

В проекте должны быть реализованы механизмы строгого контроля состава и настроек аппаратных и программных средств АСУ ТП, исключающие стихийное изменение параметров системы.

Выполнение данных требований обеспечивается за счет:

1. Разработка политики управления конфигурацией информационной (автоматизированной) системы (УКФ.0): создания регламента, определяющего эталонное состояние системы, порядок документирования настроек и периодичность проверки соответствия текущей конфигурации проектным данным.
2. Управление изменениями (УКФ.2): внедрения процедур санкционирования, тестирования

и фиксации любых изменений в ПО или аппаратной части АСУ ТП, включая ведение журналов версий и учет выполненных доработок.

3. Установка (инсталляция) только разрешенного к использованию программного обеспечения (УКФ.3): применения отечественного сертифицированного ПО, обеспечивающего контроль состава установленного софта и блокировку попыток инсталляции программ, не входящих в утвержденный «белый список» (перечень разрешенного ПО).

Примечание: В состав эксплуатационной документации должны входить регламент управления конфигурацией, перечень (эталон) разрешенного программного обеспечения и актуальные формуляры на компоненты АСУ ТП с фиксацией их версий и контрольных сумм

УПРАВЛЕНИЕ ОБНОВЛЕНИЯМИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

(ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4):

В проекте должны быть реализованы процедуры и технические решения по безопасному обновлению ПО, исключающие внесение уязвимостей и нарушение стабильности технологического процесса.

Выполнение данных требований обеспечивается за счет:

1. Разработка политики управления обновлениями программного обеспечения (ОПО.0): создания регламента, определяющего периодичность поиска обновлений, ответственных лиц, а также критичность обновлений для различных компонентов АСУ ТП.
2. Поиск, получение обновлений программного обеспечения от доверенного источника (ОПО.1): определения перечня официальных ресурсов разработчиков и проектирования защищенных каналов (или процедур офлайн-переноса) для получения дистрибутивов без прямого подключения компонентов АСУ ТП к сети «Интернет».
3. Контроль целостности обновлений программного обеспечения (ОПО.2): обязательной проверки подлинности и неизменности полученных файлов путем сверки их контрольных сумм с эталонными значениями, предоставленными разработчиком ПО.
4. Тестирование обновлений программного обеспечения (ОПО.3): проведения предварительной проверки обновлений на выделенном стенде (или тестовом сегменте), имитирующем работу реальной АСУ ТП, для подтверждения отсутствия конфликтов с технологическим ПО.
5. Установка обновлений программного обеспечения (ОПО.4): применения отечественного сертифицированного ПО для централизованного или локального развертывания проверенных обновлений в периоды планового обслуживания системы.

Примечание: в состав эксплуатационной документации должны входить регламент управления обновлениями, инструкции по проверке контрольных сумм дистрибутивов и протоколы успешного тестирования обновлений на совместимость с прикладным ПО АСУ ТП

ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

(ПЛН.0, ПЛН.1, ПЛН.2):

В проекте должна быть реализована система планирования и контроля деятельности по защите информации, обеспечивающую системный подход к безопасности АСУ ТП на всех этапах её жизненного цикла.

1. Выполнение данных требований обеспечивается за счет:
2. Разработка политики планирования мероприятий по обеспечению защиты информации (ПЛН.0): создания регламента, определяющего порядок долгосрочного и краткосрочного планирования работ по ИБ, назначение ответственных подразделений и установление целей обеспечения безопасности.
3. Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации (ПЛН.1): формирования детального графика работ (плана-графика),

включающего проведение технических проверок, инструктажей персонала, процедур продления лицензий и сертификатов на используемые средства защиты.

4. Контроль выполнения мероприятий по обеспечению защиты информации (ПЛН.2): внедрения процедур регулярной отчетности, и использования отечественного сертифицированного ПО (систем мониторинга или управления задачами) для фиксации фактов выполнения плановых работ и выявления отклонений от утвержденного графика.

Примечание: в состав эксплуатационной документации должны входить регламент планирования, типовой годовой план мероприятий по обеспечению защиты информации и формы отчетности о выполнении плановых показателей.

ОБЕСПЕЧЕНИЕ ДЕЙСТВИЙ В НЕШТАТНЫХ СИТУАЦИЯХ

(ДНС.0, ДНС.1, ДНС.2, ДНС.5, ДНС.6):

В проекте должен быть реализован комплекс организационных и технических мер, обеспечивающих готовность персонала и системы к функционированию в условиях аварийных ситуаций, сбоев или инцидентов ИБ.

Выполнение данных требований обеспечивается за счет:

1. Разработка политики обеспечения действий в нештатных ситуациях (ДНС.0): создания регламента, определяющего классификацию нештатных ситуаций, цели и задачи по обеспечению непрерывности технологического процесса и распределение полномочий сотрудников.
2. Разработка плана действий в нештатных ситуациях (ДНС.1): формирования детальных планов аварийного восстановления, содержащих алгоритмы действий по локализации угроз и переводу системы в безопасный режим функционирования.
3. Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций (ДНС.5): внедрения и настройки отечественного сертифицированного ПО для создания резервных копий конфигураций, проектов SCADA и образов, а также проектирования схем горячего или холодного резервирования аппаратных средств.
4. Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения (ДНС.6): установления процедуры обязательного технического расследования каждого случая нештатной работы системы с целью корректировки настроек средств защиты и актуализации проектных решений.

Примечание: в состав эксплуатационной документации должны входить регламент обеспечения действий в нештатных ситуациях, план аварийного восстановления (DRP), программы и методики проведения тренировок персонала, а также типовые формы актов анализа причин возникновения нештатных ситуаций

5. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ АСУ ТП И СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ (РЕКОМЕНДУЕМЫЕ)

МАШИННЫЕ

НОСИТЕЛИ

ИНФОРМАЦИИ

Машинные носители информации (внешние накопители), используемые для хранения резервных копий, должны поставляться в количестве не менее 2-х единиц на каждый тип бэкапа и удовлетворять следующим характеристикам:

- иметь ёмкость не менее 1000 ГБ (1 ТБ) для хранения полных образов системных дисков серверов, АРМ и баз данных АСУ ТП;
- иметь ёмкость не менее 100 ГБ для резервных копий конфигураций СПО, ПЛК, сетевого оборудования и средств защиты (МЭ, АВЗ);
- иметь интерфейс подключения не ниже USB 3.0 (или аналогичный по скорости передачи данных).

При выборе средств МЭ, АСО и АВЗ следует учитывать рекомендации разработчиков АСУ ТП (обязательное требование) и средства защиты, применяемые в Обществе (рекомендательное требование), при условии их соответствия требованиям по импортозамещению и наличия действующих сертификатов ФСБ и ФСТЭК России. В части обеспечения сетевой безопасности проектируемые решения должны быть технологически совместимы с существующей инфраструктурой защищенной сети ViPNet Общества (сеть №12295). Проектируемые средства защиты информации должны обеспечивать функционирование в едином ключевом пространстве и под управлением имеющихся у Общества средств централизованного управления сетью ViPNet, иметь действующие сертификаты ФСБ России по классу КС2, действующие сертификаты ФСТЭК России по 4 классу защиты.

Применение иных решений допускается при условии обеспечения полной интеграции в действующую защищенную сеть без создания параллельных систем управления и без снижения установленного уровня защищенности

Программно-технические средства защиты информации в АСУ ТП должны обеспечивать:

- Отключение всех служб и сервисов на АРМ и серверах, не используемых в процессе эксплуатации. Включение необходимых для обслуживания сервисов должно производиться временно в соответствии с регламентом управления конфигурацией;
- Программную или физическую блокировку всех неиспользуемых коммуникационных портов (USB, COM, PS/2 и др.) и интерфейсов на АРМ, серверах и сетевом оборудовании;
- Запрет загрузки ОС с внешних носителей в BIOS/UEFI всех компьютеров и серверов, а также обязательную установку пароля на изменение настроек BIOS/UEFI;
- Обязательное документирование всех параметров конфигурации АСУ ТП.

В состав эксплуатационной документации на АСУ ТП и средства защиты должны входить перечни и эталонные значения конфигурационных параметров (в том числе контрольные суммы ПО), инструкции по восстановлению защитных мер и актуальная матрица сетевых доступов.

Соглашение о финансовом контроле
*Применяется, если Договор заключен в целях реализации Концессионного соглашения и
финансируется за счет средств Капитального гранта*

_____, именуемое в дальнейшем «_____», в лице _____ действующего на основании _____, с одной стороны и _____, именуемое в дальнейшем «_____», в лице _____, действующего на основании _____, с другой стороны, составили настоящее приложение к Договору о нижеследующем:

1. Настоящее приложение составлено в целях соблюдения концессионером принятого на себя по Концессионному соглашению обязательства по обеспечению возможности контроля предоставления возмещения части расходов на строительство/реконструкцию объекта Концессионного соглашения за счет бюджетных средств (в том числе средств Капитального гранта).

2. Подписанием настоящего приложения обязанная по Договору сторона выражает свое согласие на осуществление концедентом (администрацией муниципального образования) и/или органами государственного (муниципального) финансового контроля проверок соблюдения Сторонами Договора условий, целей и порядка предоставления возмещения части расходов на строительство/реконструкцию объекта Концессионного соглашения за счет бюджетных средств (в том числе средств Капитального гранта).

Заказчик

Исполнитель

_____/_____/

М.П.

_____/_____/

М.П.

Порядок работ в части охраны окружающей среды

_____, именуемое в дальнейшем «_____», в лице _____ действующего на основании _____, с одной стороны и _____, именуемое в дальнейшем «_____», в лице _____, действующего на основании _____, с другой стороны, составили настоящее приложение к Договору о нижеследующем:

Исполнитель обязан:

1. Подготовить и представить на согласование/утверждение проектную документацию согласно перечню, предусмотренному настоящим Договором, перед направлением её на согласование/экспертизу в установленном порядке (если применимо). Представитель Заказчика, ответственный за входной контроль проектной документации, проводит проверку проектной документации в течение 10 рабочих дней со дня её получения, по истечении входного контроля Заказчик предоставляет обоснованные замечания или информирует о согласовании проектной документации. В случае неисполнения условий Договора в части предоставления проектной документации на согласование/утверждение Заказчику Исполнитель несёт бремя штрафных санкций, предусмотренных разделом 8 настоящего Договора, кроме того обязуется устранить выявленные недостатки за свой счёт в срок, согласованный с Заказчиком.

2. Самостоятельно или с привлечением сторонних организаций, имеющих разрешительную документацию, в установленном порядке подготовить и представить материалы для получения разрешительной документации на осуществление деятельности, связанной с оказанием негативного воздействия на окружающую среду и природопользованием.

3. Разработать проектную документацию в части охраны окружающей среды, оценки воздействия на окружающую среду и др. в сроки, исключающие возможность нарушения предельных сроков, установленных законодательством Российской Федерации для осуществления конкретных процедур, являющихся предметом Договора (если применимо).

4. Соблюдать действующие нормативные документы Заказчика (Стандарты, Методики, Регламенты) в области строительства.

5. Возместить Заказчику понесённые затраты, в связи с несвоевременным и (или) некачественным выполнением работ/оказанием услуг в рамках настоящего Договора в полном объёме:

- при изменении сроков начала и окончания соответствующих работ;
- при привлечении Заказчика к административной ответственности;
- при внесении Заказчиком платы за негативное воздействие на окружающую среду в повышенном размере;
- при возмещении Заказчиком вреда окружающей среде.

6. В случае обнаружения существенных недостатков результата работы Заказчик вправе предъявить Исполнителю требование о безвозмездном устранении таких недостатков, а также о возмещении понесённых Заказчиком убытков вследствие неисполнения условий Договора. К существенным недостаткам относятся недостатки товара (работы, услуги), которые делают невозможным или недопустимым использование товара (работы, услуги) в соответствии с его целевым назначением, либо которые не могут быть устранены, либо которые проявляются вновь после устранения, либо для устранения которых требуются большие затраты, либо такой(ие) недостаток(ки), который(ые) приводит(ят) к возникновению опасности для жизни, здоровья или имущества граждан и (или) Заказчика, либо вследствие которых Заказчик в значительной степени лишается того, на что он был вправе рассчитывать при заключении настоящего Договора.

7. Исполнитель в случаях, предусмотренных требованиями законодательства РФ, предъявляет Заказчику документы, подтверждающие свою компетентность и компетентность привлекаемых третьих лиц.

8. В случае привлечения третьих лиц для выполнения работ на территории Заказчика, а также предоставления территорий и (или) помещений Заказчика арендаторам, Заказчик вправе не чаще чем 1 раз в квартал проводить обследование места проведения работ и (или) арендуемой территории (помещений):

8.1. На предмет отсутствия ненадлежащего накопления и (или) размещения отходов третьим лицам, арендатором. Представитель Заказчика совместно с уполномоченными лицами Исполнителя и привлеченных третьих лиц (если применимо), арендатора осуществляют обследование территории производства работ Исполнителем или привлеченным третьим лицом, арендуемых территорий (помещений), после чего подписывают акт обследования.

В рамках обследования Заказчик вправе запросить у Исполнителя, привлеченных третьих лиц, арендатора документы, подтверждающие передачу отходов на захоронение (размещение)/обезвреживание/ утилизацию специализированной организации. В случае выявления ненадлежащего накопления и (или) размещения отходов, захламления, загрязнения территории, использования земельного участка не по его назначению Исполнитель, привлеченное третье лицо или арендатор приступает к устранению выявленных недостатков немедленно и за свой счёт.

После устранения недостатков Исполнитель, привлеченное третье лицо или арендатор сообщает Заказчику об их устранении с предъявлением подтверждающих документов при повторном обследовании территории производства работ или арендуемых помещений.

В случае неустранения выявленных недостатков в срок, согласованный с Заказчиком, Исполнитель, привлеченное третье лицо или арендатор несёт бремя штрафных санкций, предусмотренных разделом 8 настоящего Договора, кроме того обязуется устранить выявленные недостатки за свой счёт в срок, согласованный с Заказчиком.

8.2. По истечении срока аренды, а также по завершении Исполнителем или привлеченным третьим лицом предусмотренных Договором работ до подписания акта приёма-передачи выполненных работ, акта приёма-передачи территории, помещений Заказчик:

Проводит обследование места проведения работ и (или) арендуемой территории (помещений) на предмет отсутствия ненадлежащего накопления и (или) размещения отходов Исполнителем, привлеченным третьим лицом, арендатором;

Проверяет наличие у Исполнителя, привлеченного третьего лица или арендатора документов, подтверждающих передачу всех отходов, образованных в процессе деятельности на территории Заказчика, специализированным сторонним организациям для обработки/утилизации/обезвреживания/размещения.

По результатам проведения итогового обследования территории осуществления работ третьим привлеченным лицом, арендуемых территорий (помещений) составляется акт обследования, подписываемый уполномоченными лицами Заказчика третьего привлеченного лица, арендатора.

8.3. В случае выявления ненадлежащего накопления и (или) размещения отходов, захламления, загрязнения территории, использования земельного участка не по его назначению Исполнитель, третье привлеченное лицо или арендатор приступает к устранению выявленных недостатков немедленно и за свой счёт. После устранения недостатков Исполнитель, третье привлеченное лицо или арендатор сообщает Заказчику об их устранении с предъявлением подтверждающих документов при повторном обследовании территории производства работ или арендуемых помещений. Повторное обследование осуществляется Заказчиком в течение 10 рабочих дней с момента уведомления Заказчика Исполнителем об устранении недостатков. В случае отсутствия повторного обследования в течение установленного срока, недостатки считаются устраненными.

В случае неустранения выявленных недостатков в срок, согласованный с Заказчиком, Исполнитель, третье привлеченное лицо или арендатор несёт бремя штрафных санкций, предусмотренных разделом 8 настоящего Договора, кроме того обязуется устранить выявленные недостатки за свой счёт в срок, согласованный с Заказчиком.

8.4. Акт приёма-передачи выполненных работ подписывается после устранения всех недостатков, выявленных при обследовании места проведения работ и (или) арендуемой территории, а также после предъявления документов, подтверждающих обращение с отходами, образованными в рамках исполнения настоящего Договора, в соответствии с требованиями законодательства РФ (если применимо) и подписания акта приёма-передачи территории.

8.5. Подписание акта приёма-передачи Заказчиком осуществляется в случае:

Отсутствия брошенных Исполнителем, третьим привлеченным лицом, арендатором отходов вне мест их накопления/размещения, загрязнения территории нефтепродуктами и другими веществами, выявленного в результате обследования территории;

Представления Исполнителем, третьим привлеченным лицом, арендатором всех необходимых документов, подтверждающих, что образованные ими отходы переданы для обработки/утилизации/обезвреживания/размещения надлежащим образом (договоры, УПД, а также другие документы, подтверждающие проведение сделки об отчуждении отходов).

9. Если Исполнитель не представил на согласование Заказчику разрабатываемую проектную документацию, Заказчик имеет право предъявить требование Исполнителю, а Исполнитель обязуется уплатить Заказчику неустойку в размере 3% от Договорной цены, указанной в п. 4.1. Договора.

10. При ненадлежащем накоплении/размещении отходов, порче почв, а также использованию земельного участка не по назначению на месте проведения работ и (или) арендуемой территории (помещений), Заказчик имеет право предъявить требование Исполнителю, а Исполнитель обязуется уплатить Заказчику неустойку в размере 3% от Договорной цены, указанной в п. 4.1. Договора.

11. В случае начисления Исполнителю штрафов и/или неустоек в порядке и размере, установленном настоящим Договором, при оплате стоимости работ Заказчик вправе в одностороннем порядке произвести удержание части денежных средств, тем самым уменьшив стоимость оплаты по договору. В этом случае размер оплаты выполненных работ уменьшается на сумму удержания, рассчитанную в соответствии с условиями настоящего Договора.

12. В случае обнаружения существенных недостатков результата работы Заказчик вправе предъявить Исполнителю требование о безвозмездном устранении таких недостатков, а также о возмещении понесённых Заказчиком убытков вследствие неисполнения условий Договора. Заказчик выставляет Исполнителю требование о возмещении убытков на основании документов, подтверждающих факт их наличия. Исполнитель в течение 10 рабочих дней обязан компенсировать Заказчику убытки в соответствии с выставленным требованием.

Заказчик

_____/_____/

м.п.

Исполнитель

_____/_____/

м.п

Форма Плана привлечения соисполнителей из числа субъектов малого и среднего предпринимательства

*указывается наименование, фирменное наименование (при наличии), место нахождения (для юридического лица) или фамилия, имя,

№ п/п	Наименование и иные сведения о привлекаемом соисполнителе из числа субъектов малого и среднего предпринимательства*	Предмет договора, заключаемого с соисполнителем из числа СМСП, с указанием количества поставляемого им товара, объема выполняемых им работ, оказываемых им услуг	Место, условия и сроки (периоды) оказания услуг соисполнителем	Цена договора, заключаемого с соисполнителем	Срок оплаты соисполнителю за оказанные услуги**
1					
2					
ИТОГО					

отчество (при наличии), паспортные данные, место жительства (для индивидуального предпринимателя), почтовый адрес, номер контактного телефона, адрес электронной почты соисполнителя;

** не более 7 рабочих дней со дня подписания заказчиком документа о приемке оказанных услуг по договору (отдельному этапу договора).

Заказчик

_____/_____/_____
м.п.

Исполнитель

_____/_____/_____
м.п.