
Договор №
оказания услуг по сопровождению автоматизированной системы хранения данных

г. Москва

«__» _____ 2026 г.

Акционерное общество «Россети Центр инжиниринга и управления строительством Единой энергетической системы» (АО «Россети ЦИУС ЕЭС»), именуемое в дальнейшем «ЗАКАЗЧИК», в лице Заместителя генерального директора по общим вопросам Кононова Александра Николаевича, действующей на основании доверенности 13.02.2026 №1498/ХД, с одной стороны, и _____ (_____), именуемое в _____ дальнейшем ИСПОЛНИТЕЛЬ, в _____ лице _____, действующего на основании _____, с другой стороны, именуемые каждое в отдельности СТОРОНА, а при совместном упоминании – СТОРОНЫ, заключили настоящий договор оказания услуг по сопровождению автоматизированной системы хранения данных, именуемый в дальнейшем «Договор» по результатам закупочной процедуры на _____, объявленной извещением от _____ № __, на основании протокола о результатах закупочной процедуры на _____ от _____ № _____ (указывается в случае заключения договора по результатам закупочной процедуры)", о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. По настоящему Договору ЗАКАЗЧИК поручает, а ИСПОЛНИТЕЛЬ обязуется за вознаграждение:

1.1.1 оказывать услуги по сопровождению автоматизированной системы хранения данных (далее - СХД) в Исполнительном аппарате и 7 (семи) филиалах ЗАКАЗЧИКА в соответствии с Техническим заданием по сопровождению автоматизированной системы хранения данных (Приложение №1 к настоящему Договору) (далее – Услуги).

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. ЗАКАЗЧИК обязуется:

2.1.1. Принять результаты оказанных ИСПОЛНИТЕЛЕМ Услуг в случае, если они соответствуют Договору, и оплатить принятые Услуги в соответствии с Разделом 3 Договора.

2.1.2. Обеспечивать допуск представителей ИСПОЛНИТЕЛЯ в офис ЗАКАЗЧИКА (г. Москва, ул. Беловежская д. 4) для оказания Услуг по Договору, в соответствии с существующим у ЗАКАЗЧИКА порядком допуска (по заявке ИСПОЛНИТЕЛЯ).

2.1.3. Выполнять иные обязанности, предусмотренные Договором.

2.2. ЗАКАЗЧИК имеет право:

2.2.1. в любое время проверять ход исполнения Договора ИСПОЛНИТЕЛЕМ.

2.2.2. Обеспечивать получение ИСПОЛНИТЕЛЕМ всей необходимой для оказания Услуг по Договору информации (по заявке ИСПОЛНИТЕЛЯ).

2.2.3. Предоставить ИСПОЛНИТЕЛЮ по его заявке ресурсы, необходимые ему для оказания Услуг, которые определяются Договором.

2.3. ИСПОЛНИТЕЛЬ обязуется:

2.3.1. Качественно и своевременно оказывать Услуги в соответствии с условиями Договора.

2.3.2. Предоставлять ЗАКАЗЧИКУ отчётность об оказанных Услугах по Договору в соответствии с п. 4.1 Договора.

2.3.3. Соблюдать Правила внутреннего распорядка, предусмотренного на территории ЗАКАЗЧИКА.

2.3.4. Возместить ЗАКАЗЧИКУ, в полном объеме вред, причиненный имуществу ЗАКАЗЧИКА работниками ИСПОЛНИТЕЛЯ в рамках исполнения Договора, а также убытки ЗАКАЗЧИКА, возникшие вследствие нарушения ИСПОЛНИТЕЛЕМ пункта 2.4. Договора;

2.3.5. Предоставлять ЗАКАЗЧИКУ Акт сверки расчетов ежеквартально, не позднее 5 (пятого) числа месяца, следующего за отчетным кварталом.

2.3.6. Предоставлять ЗАКАЗЧИКУ информацию об изменении состава (по сравнению с существовавшим на дату заключения настоящего договора) собственников ИСПОЛНИТЕЛЯ, третьих лиц, привлеченных ИСПОЛНИТЕЛЕМ к исполнению своих обязательств по договору (состава участников; в отношении участников, являющихся юридическими лицами, - состава их участников и т.д.), включая бенефициаров (в том числе конечных), а также состава исполнительных органов ИСПОЛНИТЕЛЯ, третьих лиц, привлеченных ИСПОЛНИТЕЛЕМ к исполнению своих обязательств по договору. Информация (вместе с копиями подтверждающих документов) представляется ЗАКАЗЧИКУ по форме, указанной в Приложении № 4 к настоящему Договору, не позднее 3 календарных дней с даты наступления соответствующего события (юридического факта) способом, позволяющим подтвердить дату получения.

В случае если информация о полной цепочке собственников ИСПОЛНИТЕЛЯ, третьего лица, привлеченного ИСПОЛНИТЕЛЕМ к исполнению своих обязательств по договору, содержит персональные данные, ИСПОЛНИТЕЛЬ обеспечивает получение и направление одновременно с указанной информацией оформленных в соответствии с требованиями Федерального закона «О персональных данных» письменных согласий на обработку персональных данных, по форме, указанной в Приложении № 6 к настоящему Договору.

2.4. ИСПОЛНИТЕЛЬ гарантирует ЗАКАЗЧИКУ возможность использования полученных по Договору результатов Услуг без нарушения чьих-либо исключительных прав.

2.5. Выполнять требования Правил информационной безопасности ЗАКАЗЧИКА, утвержденных ЗАКАЗЧИКОМ (далее – Правила), в части касающейся ИСПОЛНИТЕЛЯ, а также обеспечить их исполнение от субисполнителей (в случае привлечения). В течение одного календарного дня с момента начала исполнения Договора ИСПОЛНИТЕЛЬ обязан ознакомить своих работников и работников субисполнителей (в случае привлечения) с Правилами. В случае внесения ЗАКАЗЧИКОМ изменений в Правила, ИСПОЛНИТЕЛЬ обязан руководствоваться актуальными Правилами, предоставленными ЗАКАЗЧИКОМ.

3. ЦЕНА И ПОРЯДОК ОПЛАТЫ

3.1. Общая стоимость Услуг по Договору составляет не более _____ рублей _____ копеек (_____ рублей _____ копеек), в том числе НДС _____ рублей _____ копеек (_____ рублей _____ копеек).

В случае изменения ставки НДС, общая стоимость услуг, включающая НДС и указанная в первом абзаце настоящего пункта, остается неизменной.

Ежемесячная стоимость для каждого вида Услуг по Договору определяется в соответствии с Протоколом согласования стоимости оказываемых услуг (Приложение № 2 к настоящему Договору).

3.2. Платеж за оказанные Услуги:

за отчетный период (месяц) производится ежемесячно на основании счета выставленного ИСПОЛНИТЕЛЕМ в сумме, определяемой в соответствии с ежемесячной стоимостью для каждого вида Услуг в соответствии с Протоколом согласования стоимости оказываемых услуг (Приложения № 2 к настоящему Договору) в срок не позднее 20 (двадцати) рабочих/7 (семи) рабочих* дней с момента подписания Сторонами Акта сдачи-приемки услуг по ежемесячному сопровождению СХД (Приложение № 3 к настоящему Договору) и Отчета об оказанных услугах в отчетном периоде (Приложение № 4 к

«Техническому заданию по сопровождению автоматизированной системы хранения данных» - Приложение №1 к настоящему Договору) и не должен превышать _____ рублей 00 копеек (_____ рублей __ копеек.) в том числе НДС _____ рублей __ копеек.).

**Примечание: 7-дневный срок применяется для договоров, заключаемых с субъектами малого или среднего предпринимательства.*

3.3. Обязательство ЗАКАЗЧИКА по оплате услуг считается выполненным с даты списания денежных средств с расчетного счета ЗАКАЗЧИКА.

4. ПОРЯДОК СДАЧИ-ПРИЕМКИ УСЛУГ

4.1. По окончании каждого отчетного периода (месяца) не позднее 5 числа месяца, следующего за отчетным, ИСПОЛНИТЕЛЬ передает ЗАКАЗЧИКУ подписанный со своей стороны Акт сдачи-приемки услуг по ежемесячному сопровождению СХД (Приложение № 3 к настоящему Договору) в двух экземплярах, Отчет об оказанных услугах в отчетном периоде (Приложение № 4 к «Техническому заданию по сопровождению автоматизированной системы хранения данных» - Приложение №1 к настоящему Договору), реестр инцидентов по интеграции по Форме реестра инцидентов по интеграции Приложение № 1.1 к «Техническому заданию по сопровождению автоматизированной системы хранения данных» - Приложение №1 к настоящему Договору), счет-фактуру.

4.2. ЗАКАЗЧИК в срок не позднее 10 (десяти) рабочих дней со дня получения документов, указанных в п. 4.1. Договора, при отсутствии претензий к качеству, объему или составу оказанных в отчетном периоде услуг, подписывает Акт сдачи-приемки услуг по ежемесячному сопровождению СХД и направляет один экземпляр ИСПОЛНИТЕЛЮ.

4.3. В случае, если у ЗАКАЗЧИКА имеются претензии к качеству, объему или составу оказанных в отчетном периоде услуг, а также качеству оформления документов, указанных в п. 4.1 Договора, ЗАКАЗЧИК вправе в течение 10 (десяти) рабочих дней со дня получения документов направить ИСПОЛНИТЕЛЮ мотивированный отказ от подписания Акта сдачи-приемки услуг по ежемесячному сопровождению СХД.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. ИСПОЛНИТЕЛЬ оградит ЗАКАЗЧИКА от претензий и возместит ущерб в связи с любыми убытками, ущербом, ответственностью, исками, штрафами, пенями и прочими расходами любого характера, возникшими в результате нарушений ИСПОЛНИТЕЛЕМ: обязательств по Договору, норм законодательства РФ, локальных нормативных актов ЗАКАЗЧИКА, а также связанных с отсутствием у ИСПОЛНИТЕЛЯ необходимых разрешений, лицензий, допусков. Любые расходы и затраты, связанные с несоблюдением требований Договора, действующего законодательства, нормативных документов РФ, если соблюдение этих норм зависит от ИСПОЛНИТЕЛЯ относятся исключительно на счет ИСПОЛНИТЕЛЯ.

5.2. За нарушение сроков оплаты услуг ЗАКАЗЧИКОМ ИСПОЛНИТЕЛЬ вправе потребовать уплаты неустойки в размере 1/360 ключевой ставки, установленной ЦБ РФ на день просрочки исполнения обязательства, от суммы просроченного платежа за каждый день просрочки до момента фактического исполнения обязанности по оплате.

5.3. За нарушение сроков оказания услуг по Договору ИСПОЛНИТЕЛЕМ ЗАКАЗЧИК вправе потребовать уплаты штрафных санкций, предусмотренных п. 12 таблицы «Услуга 1. Обеспечение работоспособности», п.12 таблицы «Услуга 2. Поддержка пользователей» и п. 12 таблицы «Услуга 3. Администрирование» Приложения 1 к «Техническому заданию по сопровождению автоматизированной системы хранения данных» (Приложение № 1 к настоящему Договору).

5.4. За нарушение сроков представления ИСПОЛНИТЕЛЕМ отчетных документов: Акта сдачи-приемки услуг по ежемесячному сопровождению СХД, счета-фактуры, отчета об

оказании услуг по Договору ЗАКАЗЧИК вправе потребовать уплаты пени в размере 0,1% от стоимости услуг в отчетном периоде за каждый день просрочки.

5.5. ИСПОЛНИТЕЛЬ в полной мере несет ответственность за действия и бездействие своего Персонала, любого из привлеченных ИСПОЛНИТЕЛЕМ третьих лиц, их персонала или агентов, как если бы это были его собственные действия или бездействие.

5.6. Антикоррупционная оговорка.

5.6.1. ИСПОЛНИТЕЛЮ известно о том, что ЗАКАЗЧИК реализует требования статьи 13.3 Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции», принимает меры по предупреждению коррупции, ведет антикоррупционную политику и развивает не допускающую коррупционных проявлений культуру, поддерживает деловые отношения с контрагентами, которые гарантируют добросовестность своих партнеров и поддерживают антикоррупционные стандарты ведения бизнеса.

5.6.2. ИСПОЛНИТЕЛЬ настоящим подтверждает, что он ознакомился с Антикоррупционной политикой ЗАКАЗЧИКА (представленной в разделе «Антикоррупционная политика» на официальном сайте ЗАКАЗЧИКА по адресу: <http://www.ci-us-ees.ru>), полностью принимает положения Антикоррупционной политики ЗАКАЗЧИКА и обязуется обеспечивать соблюдение ее требований как со своей стороны, так и со стороны аффилированных с ним физических и юридических лиц, действующих по настоящему Договору, включая собственников, должностных лиц, работников и/или посредников.

5.6.3. При исполнении своих обязательств по настоящему 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 или достичь иных неправомерных целей.

Стороны отказываются от стимулирования каким-либо образом работников друг друга, в том числе путем предоставления денежных сумм, подарков, безвозмездного выполнения для них работ (оказания услуг) и другими, не поименованными здесь способами, ставящими работника в определенную зависимость и направленными на обеспечение выполнения этим работником каких-либо действий в пользу стимулирующей его стороны (ИСПОЛНИТЕЛЯ и ЗАКАЗЧИКА).

5.6.4. В случае возникновения у одной из Сторон подозрений, что произошло или может произойти нарушение каких-либо положений пунктов 5.6.1 – 5.6.3 настоящего Договора, указанная Сторона обязуется уведомить об этом другую Сторону в письменной форме. После письменного уведомления Сторона имеет право приостановить исполнение настоящего Договора до получения подтверждения, что нарушения не произошло или не произойдет. Это подтверждение должно быть направлено в течение 10 (десяти) рабочих дней с даты направления письменного уведомления.

В письменном уведомлении Сторона обязана сослаться на факты и/или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений п. 5.6.1, п. 5.6.2 настоящего Договора любой из Сторон, аффилированными лицами, работниками или посредниками.

5.6.5. В случае нарушения одной из Сторон обязательств по соблюдению требований, предусмотренных п. 5.6.1 и п. 5.6.2 настоящего Договора, и обязательств воздерживаться от запрещенных п. 5.6.3 настоящего Договора действий и/или неполучения другой Стороной в установленный срок подтверждения, что нарушения не произошло или не произойдет, Сторона имеет право расторгнуть настоящий Договор в одностороннем порядке полностью или в части, направив письменное уведомление о расторжении. Сторона, по чьей инициативе был расторгнут настоящий Договор, в соответствии с положениями настоящего пункта

вправе требовать возмещения реального ущерба, возникшего в результате такого расторжения.

5.7. В части, не урегулированной Договором, Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

5.8. За несоблюдение ИСПОЛНИТЕЛЕМ обязательств, предусмотренных Правилами (пункт 2.5 Договора), ИСПОЛНИТЕЛЬ обязан уплатить штраф в размере 100 000 (сто тысяч) рублей 00 копеек за каждый случай неисполнения или ненадлежащего исполнения указанных обязательств, а также полностью возместить ЗАКАЗЧИКУ убытки, причиненные таким нарушением обязательств в полной сумме сверх суммы штрафа.

5.9. Налоговая оговорка.

5.9.1. ИСПОЛНИТЕЛЬ гарантирует, что:

- зарегистрирован в ЕГРЮЛ надлежащим образом;
- его исполнительный орган находится и осуществляет функции управления по месту регистрации юридического лица, и в нем нет дисквалифицированных лиц;
- располагает персоналом, имуществом и материальными ресурсами, необходимыми для выполнения своих обязательств по Договору, а в случае соисполнителей принимает все меры должной осмотрительности, чтобы соисполнители соответствовали данному требованию;
- располагает лицензиями, необходимыми для осуществления деятельности и исполнения обязательств по Договору, если осуществляемая по Договору деятельность является лицензируемой;
- является членом саморегулируемой организации, если осуществляемая по Договору деятельность требует членства в саморегулируемой организации;
- ведет бухгалтерский учет и составляет бухгалтерскую отчетность в соответствии с законодательством Российской Федерации и нормативными правовыми актами по бухгалтерскому учету, представляет годовую бухгалтерскую отчетность в налоговый орган;
- ведет налоговый учет и составляет налоговую отчетность в соответствии с законодательством Российской Федерации, субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления, своевременно и в полном объеме представляет налоговую отчетность в налоговые органы;
- не допускает искажения сведений о фактах хозяйственной жизни (совокупности таких фактов) и объектах налогообложения в первичных документах, бухгалтерском и налоговом учете, в бухгалтерской и налоговой отчетности, а также не отражает в бухгалтерском и налоговом учете, в бухгалтерской и налоговой отчетности факты хозяйственной жизни выборочно, игнорируя те из них, которые непосредственно не связаны с получением налоговой выгоды;
- своевременно и в полном объеме уплачивает налоги, сборы и страховые взносы;
- отражает в налоговой отчетности по НДС все суммы НДС, предъявленные ЗАКАЗЧИКУ;
- лица, подписывающие от его имени первичные документы и счета-фактуры, имеют на это все необходимые полномочия и доверенности;
- информирует ЗАКАЗЧИКА о признании ИСПОЛНИТЕЛЯ банкротом, в срок не позднее 10 (десяти) рабочих дней, с даты вступления в законную силу решения арбитражного суда.

5.9.2. Если ИСПОЛНИТЕЛЬ нарушит гарантии (любую одну, несколько или все вместе), указанные в пункте 5.9.1. настоящего Договора, и это повлечет:

- предъявление налоговыми органами требований к ЗАКАЗЧИКУ об уплате налогов, сборов, страховых взносов, штрафов, пеней, отказ в возможности признать расходы для целей налогообложения прибыли или включить НДС в состав налоговых вычетов и(или)
- предъявление третьими лицами, купившими у ЗАКАЗЧИКА товары (работы, услуги), имущественные права, являющиеся предметом настоящего Договора, требований к ЗАКАЗЧИКУ о возмещении убытков в виде начисленных по решению налогового органа

налогов, сборов, страховых взносов, пеней, штрафов, а также возникших из-за отказа в возможности признать расходы для целей налогообложения прибыли или включить НДС в состав налоговых вычетов,

ИСПОЛНИТЕЛЬ обязуется возместить **ЗАКАЗЧИКУ** убытки, которые последний понес вследствие таких нарушений.

5.9.3. **ИСПОЛНИТЕЛЬ** в соответствии со ст. 406.1 Гражданского кодекса Российской Федерации, возмещает **ЗАКАЗЧИКУ** все убытки последнего, возникшие в случаях, указанных в пункте 5.9.2 настоящего Договора. При этом факт оспаривания или неоспаривания налоговых доначислений в налоговом органе, в том числе вышестоящем, или в суде, а также факт оспаривания или неоспаривания в суде претензий третьих лиц не влияет на обязанность **ИСПОЛНИТЕЛЯ** возместить имущественные потери **ЗАКАЗЧИКА**.

5.9.4. **ИСПОЛНИТЕЛЬ** обязан в течение 5 рабочих дней с момента получения соответствующей претензии от **ЗАКАЗЧИКА** возместить **ЗАКАЗЧИКУ** имущественные потери путём перечисления денежных средств на его расчетный счет.

6. СРОК ДЕЙСТВИЯ, ИЗМЕНЕНИЕ И РАСТОРЖЕНИЕ ДОГОВОРА

6.1. Договор вступает в силу с момента его подписания и действует до полного исполнения Сторонами обязательств.

Срок оказания услуг по Договору – 24 месяца с даты подписания настоящего Договора.

6.2. **ЗАКАЗЧИК** в любое время имеет право в одностороннем порядке расторгнуть Договор, уведомив об этом Исполнителя за 10 дней до предполагаемой даты расторжения Договора, при неисполнении либо ненадлежащем исполнении Исполнителем следующих обязанностей по Договору:

6.2.1. Срыв **ИСПОЛНИТЕЛЕМ** начала оказания услуг более чем на 10 (десять) дней по причинам, не зависящим от **ЗАКАЗЧИКА**.

6.2.2. Несоблюдение **ИСПОЛНИТЕЛЕМ** требований по качеству услуг, если исправление нарушений займет более чем 10 (десять) дней.

6.2.3. Неоднократное (2 и более раз) нарушение **ИСПОЛНИТЕЛЕМ** установленных сроков выполнения Услуг.

6.3. Договор также может быть расторгнут досрочно в следующих случаях:

6.3.1. По соглашению Сторон, оформленному дополнительным соглашением, подписанным уполномоченными представителями Сторон.

6.3.2. На основании решения суда по иску заинтересованной Стороны.

6.3.3. При ликвидации одной из Сторон как юридического лица либо ограничение его уставной правоспособности в законном порядке, если данное обстоятельство влечет для этой Стороны невозможность выполнять свои обязательства по Договору.

6.3.4. В случае неисполнения **ИСПОЛНИТЕЛЕМ** обязанностей, установленных п. 2.3.6. настоящего Договора, **ЗАКАЗЧИК** вправе в одностороннем внесудебном порядке без возмещения **ИСПОЛНИТЕЛЮ** убытков отказаться от исполнения настоящего Договора, письменно уведомив об этом **ИСПОЛНИТЕЛЯ**. Договор считается расторгнутым по истечении 5 (пяти) календарных дней с момента получения **ИСПОЛНИТЕЛЕМ** указанного письменного уведомления **ЗАКАЗЧИКА**.

7. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

7.1. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств по настоящему Договору, если такое неисполнение или ненадлежащее исполнение явилось следствием обстоятельств непреодолимой силы, т.е. чрезвычайных и непредотвратимых при данных условиях обстоятельств. К таким обстоятельствам относятся: наводнение, землетрясение, ураган, взрыв, пожар, шторм, общественные беспорядки, военные действия, восстание и др.

7.2. В случае возникновения обстоятельств непреодолимой силы Сторона,

ссылающаяся на действие обстоятельств непреодолимой силы, обязана:

7.2.1. Немедленно в письменной форме известить другую Сторону об их наступлении и предоставить подтверждение их наличия.

7.2.2. Предпринять необходимые действия для уменьшения последствий обстоятельств непреодолимой силы и устранения препятствий к исполнению обязательств по Договору.

7.2.3. Уведомить другую Сторону о возобновлении выполнения своих обязательств по Договору по окончании действия обстоятельств непреодолимой силы.

7.3. Отсутствие уведомления или несвоевременное уведомление лишает сторону права ссылаться на обстоятельства непреодолимой силы как на основание, освобождающее ее от ответственности за неисполнение обязательств по настоящему Договору.

7.4. При наличии обстоятельств непреодолимой силы сроки выполнения Сторонами обязательств по настоящему Договору отодвигаются соразмерно времени, в течение которого действуют обстоятельства непреодолимой силы, либо соразмерно времени, необходимого для устранения последствий действия таких обстоятельств. В случае, если обстоятельства непреодолимой силы продолжаются свыше 3 месяцев подряд, либо сроки, требующиеся для устранения Сторонами последствий действия таких обстоятельств, превышают 3 месяца, Стороны проводят переговоры на предмет возможности продолжения договорных отношений, либо подписывают соглашение о расторжении Договора.

8. РАЗРЕШЕНИЕ СПОРОВ

8.1. Все споры и разногласия, возникающие при заключении и исполнении Договора, разрешаются, путем переговоров и направления Сторонами претензий. Стороны устанавливают обязательный досудебный (претензионный) порядок разрешения споров. Претензии по фактам неисполнения (ненадлежащего исполнения) Договора должны быть оформлены в письменном виде и подлежат рассмотрению в срок не более 15 дней с даты получения.

8.2. В случае невозможности разрешения споров путем переговоров Стороны после реализации процедуры досудебного урегулирования разногласий передают их на рассмотрение Арбитражного суда г. Москвы.

9. КОНФИДЕНЦИАЛЬНОСТЬ

9.1. ИСПОЛНИТЕЛЬ не вправе раскрывать третьим лицам предоставляемую ЗАКАЗЧИКОМ юридическую, финансовую и иную информацию, связанную с заключением и исполнением Договора, в случае, если ИСПОЛНИТЕЛЬ, получивший такую информацию, заранее поставлен в известность, что для предоставившего такую информацию ЗАКАЗЧИКА она является служебной или коммерческой тайной либо по иным причинам эта информация не должна раскрываться.

9.2. ИСПОЛНИТЕЛЬ обязуется:

9.2.1. Обеспечить хранение конфиденциальной информации, исключаящее доступ к информации третьих лиц.

9.2.3. Не передавать конфиденциальную информацию третьим лицам, как в полном объеме, так и частично.

9.3. ИСПОЛНИТЕЛЬ вправе по согласованию с ЗАКАЗЧИКОМ привлекать для оказания услуг третьих лиц при условии сохранения конфиденциальности получаемой от ЗАКАЗЧИКА информации, при этом ИСПОЛНИТЕЛЬ несет ответственность за действия (бездействие) таких лиц, как за свои собственные.

9.4. Заявления для печати или иные публичные заявления ИСПОЛНИТЕЛЯ, связанные с условиями Договора, требуют предварительного письменного согласия ЗАКАЗЧИКА.

9.5. Предусмотренные настоящим разделом Договора обязательства в отношении конфиденциальной информации действуют в течение 5 лет после прекращения действия

Договора.

9.5.1. Порядок передачи и охраны информации, составляющей коммерческую тайну, определяется «Соглашением о передаче и охране информации, составляющей коммерческую тайну» (Приложение № 5 к настоящему Договору).

10. ПРОЧИЕ УСЛОВИЯ

10.1 Ни одна из Сторон Договора не имеет права передавать свои права и обязанности третьей Стороне без письменного согласия другой Стороны.

10.2 Все уведомления и иные документы, которые должны либо могут быть направлены в рамках Договора или в связи с его исполнением, должны быть направлены с нарочным, либо заказным письмом с уведомлением о вручении соответственно в адреса, указанные в статье 11 настоящего Договора.

10.3 После подписания Договора все предыдущие письменные и устные соглашения, переписка, переговоры между Сторонами, относящиеся к данному Договору, теряют силу, если они противоречат Договору.

10.4 Реорганизация любой из Сторон не является основанием для изменения условий или расторжения Договора. В этом случае Договор сохраняет силу для правопреемников Сторон.

10.5 Все изменения и дополнения к Договору, а также любые договорённости между Сторонами, влекущие за собой новые обстоятельства, которые вытекают из Договора, считаются действительными, если они оформлены в письменном виде и подписаны Сторонами в форме дополнений или изменений к Договору.

10.6 Во всем ином, что не предусмотрено Договором, Стороны будут руководствоваться действующим законодательством Российской Федерации.

10.7 Договор составлен в двух экземплярах на русском языке, каждый из которых имеет одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

10.8 К Договору прилагаются и являются его неотъемлемой частью:

- Приложение №1: Техническое задание по сопровождению автоматизированной системы хранения данных;
- Приложение №2: Протокол согласования стоимости оказываемых услуг;
- Приложение №3: Форма Акта сдачи-приемки услуг по ежемесячному сопровождению СХД;
- Приложение №4: Форма справки о цепочке собственников;
- Приложение №5: Соглашение о передаче и охране информации, составляющей коммерческую тайну;
- Приложение №6: Форма согласия на обработку персональных данных.

10.9 Настоящим Исполнитель подтверждает, что ознакомлен с Правилами информационной безопасности Заказчика.

Подпись: _____ (_____)*

11. РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

ЗАКАЗЧИК:

АО «Россети ЦИУС ЕЭС»

ИНН 7728645409

КПП 774550001

Юридический адрес:

121353, г. Москва, вн.тер.г.

муниципальный округ Можайский, ул.

Беловежская, д. 4

Почтовый адрес: 121353, г. Москва,

ИСПОЛНИТЕЛЬ:

вн.тер.г. муниципальный округ
Можайский, ул. Беловежская, д. 4
Тел/факс +7 (495)710-60-60
адрес электронной почты cius@fsk-ees.ru
р/с 40702810738120011798
в ПАО Сбербанк г. Москва
к/с 30101810400000000225
БИК 044525225

АО «Россети ЦИУС ЕЭС»

_____ / _____ /

_____ / _____ /

Приложение №1
к Договору № _____
от _____

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

по сопровождению автоматизированной системы хранения данных

СОДЕРЖАНИЕ

ДОГОВОР №.....	1
1. ОБЩИЕ СВЕДЕНИЯ.....	12
1.1. ТЕРМИНЫ, СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ.....	12
1.2. ЗАКАЗЧИК И ИСПОЛНИТЕЛЬ.....	15
1.3. ПОЛНОЕ И КРАТКОЕ НАИМЕНОВАНИЕ УСЛУГ.....	15
1.4. МЕСТО И СРОКИ ОКАЗАНИЯ УСЛУГ.....	16
2. ХАРАКТЕРИСТИКА УСЛУГ.....	16
2.1. ОБЪЕКТЫ УСЛУГ.....	16
2.2. ЦЕЛИ ОКАЗАНИЯ УСЛУГ.....	16
2.3. РЕЗУЛЬТАТЫ ОКАЗАНИЯ УСЛУГ.....	16
2.4. ОБЩИЕ ТРЕБОВАНИЯ К КАЧЕСТВУ УСЛУГ.....	16
3. ОБЩИЕ ТРЕБОВАНИЯ К УСЛУГАМ.....	17
3.1. ОСНОВНЫЕ СТАНДАРТЫ НЕПРЕРЫВНОСТИ ОБЪЕКТОВ УСЛУГ ПО КЛАССАМ КРИТИЧНОСТИ.....	17
3.2. ТРЕБОВАНИЯ К РЕЖИМАМ РАБОТЫ ОБЪЕКТОВ УСЛУГ.....	18
3.3. ОГРАНИЧЕНИЯ В ЧАСТИ ОКАЗАНИЯ УСЛУГ.....	18
3.4. ПЕРЕЧЕНЬ ОБЪЕКТОВ УСЛУГ.....	19
3.5. ТРЕБОВАНИЯ К ЧИСЛЕННОСТИ И КВАЛИФИКАЦИИ ПЕРСОНАЛА ИСПОЛНИТЕЛЯ.....	21
4. ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ.....	22
4.1. ТРЕБОВАНИЕ К ДОКУМЕНТАЦИОННОМУ ОБЕСПЕЧЕНИЮ.....	22
4.2. ТРЕБОВАНИЯ К ОРГАНИЗАЦИОННОМУ ОБЕСПЕЧЕНИЮ.....	22
5. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	22
5.1. ОБЩИЕ ТРЕБОВАНИЯ.....	22
5.2. ТРЕБОВАНИЯ К АРМ СПЕЦИАЛИСТОВ ИСПОЛНИТЕЛЯ.....	23
6. ПЕРЕЧЕНЬ И ПОРЯДОК ОКАЗАНИЯ УСЛУГ.....	23
6.1. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ УСЛУГ.....	23
6.2. ПОРЯДОК ОКАЗАНИЯ УСЛУГ.....	23
7. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ.....	23
1 ПРИЛОЖЕНИЕ 1. ПЕРЕЧЕНЬ И СОДЕРЖАНИЕ УСЛУГ.....	25
1. ОБЪЕКТ УСЛУГ: АВТОМАТИЗИРОВАННАЯ СИСТЕМА ХРАНЕНИЯ ДАННЫХ (СХД).....	25
1.1. Компонентный состав.....	25
1.2. Зона охвата Услуг.....	28
1.3. Карточки Услуг.....	29
Услуга 1. Обеспечение работоспособности.....	29
Услуга 2. Поддержка Пользователей.....	33
Услуга 3. Администрирование.....	34
ФОРМА РЕЕСТРА ИНЦИДЕНТОВ ПО ИНТЕГРАЦИИ.....	39
2 ПРИЛОЖЕНИЕ 2. ПЕРЕЧЕНЬ ПЕРЕДАВАЕМЫХ ДОКУМЕНТОВ.....	40
3 ПРИЛОЖЕНИЕ 3. ПОРЯДОК ОКАЗАНИЯ УСЛУГ.....	41
1. Общие положения.....	41
2. Термины, определения и сокращения.....	41
3. Обязанности Исполнителя.....	41
4. Обязанности Заказчика.....	42
5. Ответственные лица.....	42
6. Обработка заявок.....	42
7. Проведение плановых и аварийных работ.....	46
4 ПРИЛОЖЕНИЕ 4. ФОРМЫ ОТЧЁТНЫХ ДОКУМЕНТОВ.....	48
Форма 1. Сводный отчёт по объёму оказанных Услуг.....	48

	Форма 2. Детальный отчёт по заявкам Пользователей за период с ____ по ____ 49	
5	ПРИЛОЖЕНИЕ 5. ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	50
1.	ОБЩИЕ ПОЛОЖЕНИЯ.....	54
2.	ПРАВИЛА РАБОТЫ С ИНФОРМАЦИЕЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА.....	55
3.	ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ / ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ.....	56
4.	ПРАВИЛА РАБОТЫ С УЧЕТНЫМИ ЗАПИСЯМИ.....	57
5.	ПРАВИЛА РАБОТЫ С ПАРОЛЯМИ.....	58
6.	ПРАВИЛА РАБОТЫ НА АРМ.....	60
7.	ПРАВИЛА РАБОТЫ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ.....	63
8.	ПРАВИЛА РАБОТЫ В ЛВС.....	64
9.	ПРАВИЛА РАБОТЫ В СЕТИ ИНТЕРНЕТ.....	65
10.	ПРАВИЛА РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ.....	67
11.	ПРАВИЛА РАБОТЫ С НОСИТЕЛЯМИ ИНФОРМАЦИИ.....	68
12.	ПРАВИЛА РАБОТЫ С НОСИТЕЛЯМИ КЛЮЧЕВОЙ ИНФОРМАЦИИ.....	69
13.	ПРАВИЛА РАБОТЫ С СИСТЕМАМИ ДБО.....	70
14.	КОНТРОЛЬ.....	71
15.	ОТВЕТСТВЕННОСТЬ.....	73
	АО «РОССЕТИ ЦЕНТР ИНЖИНИРИНГА И УПРАВЛЕНИЯ СТРОИТЕЛЬСТВОМ ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ».....	84
	ОБЛАДАТЕЛЬ ИНФОРМАЦИИ.....	84
	КОНТРАГЕНТ.....	84
	Я, _____.....	85
	ОБЛАДАТЕЛЬ ИНФОРМАЦИИ.....	85
	КОНТРАГЕНТ.....	85
	ФОРМА.....	86
	Согласие на обработку персональных данных.....	86

1. Общие сведения

1.1. Термины, сокращения и определения

Термины, сокращения и определения

Сокращение, термин	Расшифровка сокращения, определение
АВПО	Антивирусное ПО.
Аппаратные компоненты	Тип компонентов Объекта Услуг, включающий категории Аппаратная ИВИ (серверное оборудование, сетевое оборудование, СХД), Прочее оборудование (ВКС, телефония).
АРМ	Автоматизированное рабочее место.
АСУИИиК	Автоматизированная система управления инцидентами, изменениями и конфигурациями, САСП Исполнителя.
БД	База данных.
Версия ПО	Официально выпущенная версия ПО, имеющая определенный порядковый номер.
Время реакции	Интервал времени между моментом назначения заявки Специалистом САСП на Специалиста Службы технической поддержки Исполнителя и переводом заявки в работу.
Время решения	Время, в течение которого Служба технической поддержки Исполнителя должна решить Заявку пользователя Объекта Услуг и описать решение без учёта времени уточнения у пользователя недостающей для решения запроса информации. Выполнение заявки также может откладываться (приостанавливаться) по другим, не зависящим от Исполнителя, причинам, из-за отсутствия пользователя или его неготовности к проведению необходимых работ.
День	В настоящем ТЗ днём называется день Рабочего времени, если явно не указано иное.
Договор	Договор оказания услуг по сопровождению автоматизированной системы хранения данных, к которому данное ТЗ является неотъемлемым приложением.
Заказчик	Акционерное общество «Россети Центр инжиниринга и управления строительством Единой энергетической системы» (АО «Россети ЦИУС ЕЭС».
Запрос на обслуживание (ЗНО)	Запрос пользователя Объекта Услуг на информацию, консультацию или действие по управлению доступом к функциям и данным Объекта Услуг, который не связан с возникновением сбоя в работе Объекта Услуг или необходимостью внесения изменений в Объект Услуг.

Заявка	Обращение, составляемое пользователем Объекта Услуг и передаваемое в САСП с целью дальнейшего получения Услуг от Исполнителя.
Злонамеренное действие	Умышленное деяние, направленное на нанесение ущерба Заказчику.
ИБ	Информационная безопасность.
ИВИ	Информационно-вычислительная инфраструктура.
Инженерные компоненты	Тип компонентов Объекта Услуг, включающий категорию Инженерные системы (система электропитания, система охлаждения, система пожаротушения, СКУД, прочие инженерные системы ЦОД).
Информационная система	Программное или программно-аппаратное решение Заказчика, предназначенное для автоматизации деятельности одного или нескольких подразделений.
Инцидент	Незапланированное прерывание или снижение качества работы Объекта Услуг.
ИС	Информационная система.
Исполнитель	Исполнитель по договору оказания услуг по сопровождению автоматизированной системы хранения данных - определяется в результате конкурсных процедур (указывается при заключении договора).
ИТ	Информационные технологии.
ИТ-решение	Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализованная посредством ИТ.
ИТС	Информационно-телекоммуникационная сеть.
КСПД	Корпоративная сеть передачи данных.
Несанкционированные изменения	Изменения, внесенные без согласования со стороны функционального заказчика, в том числе, без наличия соответствующего обращения от пользователя Объекта Услуг.
НСИ	Нормативно-справочная информация.
Обновление Объекта Услуг	Новая версия Объекта Услуг, предназначенная для установки взамен либо в дополнение к существующей версии, в которой устранены выявленные дефекты ПО или выполнена доработка отдельных функций, направленная на повышение производительности или удобство эксплуатации.
Объект Услуг	Объект, в отношении которого оказываются Услуги сопровождения в соответствии с настоящим ТЗ. Объекты Услуг

	могут быть следующих видов: • ИТ-решение, внедрённая ИС, принадлежащая Заказчику, поставленная на баланс, переведённая в ПЭ; • ПО, приобретённое и установленное на АРМ Заказчика, при этом не являющееся ИС; • ИТ-оборудование, приобретённое, поставленное на баланс и эксплуатируемое Заказчиком; • Сервис, предоставляемый Заказчику в качестве ИТ-услуги, например доступ к ИТ-решению стороннего провайдера ИТ-услуг или предоставляемое в аренду ИТ-оборудование.
Опротестованная заявка	Заявка Заказчика, не принятая им после исполнения, обоснованно возвращённая на доработку.
ОС	Операционная система.
ОЭ	Опытная эксплуатация.
ПМИ	Программа и методика испытаний.
ПО	Программное обеспечение.
Пользователь	Сотрудники Заказчика, использующие Объект Услуг в служебных целях. Также пользователями могут выступать сотрудники сторонних организаций, контрагентов Заказчика.
Порядок	Порядок оказания Услуг, являющийся приложением к настоящему ТЗ.
ППО	Прикладное программное обеспечение.
Программные компоненты	Тип компонентов Объекта Услуг, включающий категории: Прикладное ПО (пользовательские интерфейсы, прикладные подсистемы и модули, расчетные алгоритмы), Системное ПО (операционные системы, системы контейнеризации, СУБД, системные службы, серверы приложений, прочее системное ПО), Виртуальная ИВИ (системы виртуализации, виртуальные серверы, виртуальные сети, виртуальные СХД, виртуальные порты доступа).
ПСИ	Приёмо-сдаточные испытания.
ПЭ	Промышленная эксплуатация.
Рабочее время	С 05:00 до 18:00 (GMT+3)
САСП	Система автоматизации службы поддержки пользователей. В соответствии с настоящим ТЗ используется система Исполнителя.
Сбой	Потеря Объектом Услуг или его частью способности функционировать в соответствии с эксплуатационной документацией или предоставить требуемый результат. Сбой часто служит причиной Инцидента.
Системное ПО	Системное программное обеспечение - ПО, необходимое для обеспечения функционирования сервера или АРМ (ОС,

	необходимые драйверы).
СКУД	Система контроля учёта доступа.
Служба технической поддержки	Структурное или функциональное подразделение Исполнителя, предназначенное для оказания Услуг сопровождения Объекта Услуг в процессе его эксплуатации Пользователям.
Соглашение	Соглашение об уровне Услуг, Service Level Agreement (SLA), в котором определены целевые показатели качества услуг.
Специалист Службы технической поддержки	Сотрудник Исполнителя, который осуществляет рассмотрение, анализ и обработку поступающих заявок Пользователей в Службу технической поддержки.
Стороны	Совместно Заказчик и Исполнитель.
СУБД	Система управления базами данных.
СХД	Система хранения данных.
ТЗ	Техническое задание.
Услуги	Услуги, оказываемые в соответствии с условиями договора, в т.ч. данного ТЗ.
Фиктивная заявка	Заявка, самостоятельно и необоснованно созданная сотрудниками Исполнителя без согласования Заказчика.
Функциональный заказчик	Одно или несколько подразделений Заказчика.
Час	В настоящем ТЗ часом называется один час Рабочего времени, если явно не указано иное.
Эксплуатационная документация	Руководство пользователя и Руководство администратора, предоставляемые Исполнителем

1.2. Заказчик и Исполнитель

1.2.1. Заказчик: АО «Россети ЦИУС ЕЭС».

1.2.2. Исполнитель: _____ (**определяется в результате конкурсных процедур (указывается при заключении договора оказания услуг по сопровождению автоматизированной системы хранения данных)*).

1.3. Полное и краткое наименование Услуг

1.3.1. Полное наименование: Услуги по сопровождению автоматизированной системы хранения данных АО «Россети ЦИУС ЕЭС» (далее – СХД) в Исполнительном аппарате и 7 (семи) филиалах Заказчика.

1.3.2. Краткое наименование: Услуги.

1.4. Место и сроки оказания Услуг

1.4.1. Место оказания Услуг: г. Москва, ул. Беловежская д. 4. По согласованию с Заказчиком услуги могут оказываться в удаленном режиме с соблюдением Правил информационной безопасности АО «Россети ЦИУС ЕЭС». В случае наличия/введения ограничений (в том числе временных) по предоставлению

удаленного доступа к информационным ресурсам Заказчика, Исполнитель организует присутствие в офисе Заказчика специалистов, в зависимости от специфики возникающих задач, в рамках исполнения Договора. Оказание услуг Исполнителем в удаленном режиме не может носить постоянных характер и, по согласованию с Заказчиком, требует исполнения части работ в офисе Заказчика.

1.4.2. Сроки оказания Услуг: в течение 24 месяцев с даты заключения договора.

2. Характеристика Услуг

2.1. Объекты Услуг

2.1.1. Объектами Услуг являются Информационные системы Заказчика, указанные в п.3.4.

2.2. Цели оказания Услуг

2.2.1. Целями оказания Услуг являются:

- обеспечение непрерывности бизнес-процессов Заказчика, автоматизация которых осуществляется с использованием Объектов Услуг, включенных в ТЗ.

2.3. Результаты оказания Услуг

2.3.1. Результатами оказания Услуг являются:

- Объекты Услуг, функционирующие с соблюдением требований надежности в соответствии со степенью критичности для каждого Объекта Услуг;
- отработанные с соблюдением условий Соглашения заявки Пользователей;
- решённые с соблюдением условий Соглашения инциденты и устранённые сбои в работе Объектов Услуг;

2.4. Общие требования к качеству Услуг

2.4.1. Качество оказываемых Исполнителем Услуг должно соответствовать требованиям действующего законодательства Российской Федерации и условиям заключенного Договора.

2.4.2. Общие требования к качеству оказываемых Исполнителем Услуг определены положениями следующих государственных стандартов:

- ГОСТ ИСО 9001-2015. «Системы менеджмента качества. Требования»;
- ГОСТ 34.201-2020. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем»;
- ГОСТ Р 59793-2021. «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- ГОСТ Р 57193-2016. «Информационная технология. Системная инженерия. Процессы жизненного цикла систем»;
- ГОСТ Р ИСО/МЭК 14764-2002. «Информационная технология. Сопровождение программных средств».

2.4.3. Дополнительные и специальные требования к порядку, условиям и качеству оказания Исполнителем Услуг содержатся в карточках услуг в приложении 1 к настоящему ТЗ.

2.4.4. При оказании Услуг Исполнитель обязан соблюдать внутренние регламенты и процедуры, утверждённые Заказчиком. Документы с описанием

соответствующих регламентов и процедур, не включенных в объем передаваемых документов в соответствии с условиями ТЗ, предоставляются по требованию Исполнителя в согласованные сторонами сроки. Перечень передаваемых Заказчиком Исполнителю документов, необходимых для оказания Услуг, указан в приложении 2.

3. Общие требования к Услугам

3.1. Основные стандарты непрерывности Объектов Услуг по классам Критичности

3.1.1. В отношении Объектов Услуг установлены следующие требования в части соответствия основным стандартам непрерывности по классам Критичности:

- К-1, критически важные – Объекты Услуг, работающие непрерывно в режиме «боевого дежурства», выход из строя которых влечёт за собой невосполнимые потери для бизнеса, в т.ч. угрозу жизни и здоровью персонала и населения;
- К-2, критические для бизнеса – критические для управления организацией Заказчика Объекты Услуг, как правило, с непрерывным режимом работы, выход из строя которых влечёт за собой значительные потери и ущерб для Заказчика;
- К-3, важные для бизнеса – обычные Объекты Услуг, с режимом работы, соответствующим Рабочему времени Заказчика;
- К-4, поддерживающие – не критические для управления организацией Заказчика Объекты Услуг, в случае отказа которых организация Заказчика остается способным осуществлять свою основную деятельность без заметной потери качества.

3.1.2. Основные стандарты непрерывности Объектов Услуг по классам Критичности, принятые у Заказчика, приведены в таблице ниже. Время указано календарное.

Класс Критичности

№ п/п	Наименование характеристики	Классификация критичности Объекта Услуг			
		Критически важные (К-1)	Критические для бизнеса (К-2)	Важные для бизнеса (К-3)	Поддерживающие (К-4)
1	Целевая доступность	99,96%	99,73%	99,20%	98,00%
2	Внеплановые простои в месяц, не более	~18 мин	~2 ч	~6 ч	~14 ч
3	Время восстановления (RTO), не более	30 мин	4 ч	24 ч	72 ч
4	Период потери данных (RPO), не более	0 мин	8 ч	24 ч	24 ч
5	Требуемый режим работы системы	Непрерывно	Непрерывно	Рабочее время	Рабочее время
6	Доступность ИТ специалистов	Непрерывно	Круглосуточно в рабочие дни	Рабочее время	Рабочее время

3.2. Требования к режимам работы Объектов Услуг

3.2.1. Определены следующие режимы работы Объектов Услуг:

- штатный;
- аварийный;
- режим обслуживания.

3.2.2. Основным режимом является штатный режим. В этом режиме работают все настроенные функции Объекта Услуг.

3.2.3. Аварийный режим работы характеризуется отказом одной или нескольких функций Объекта Услуг.

3.2.4. Режим обслуживания должен использоваться для выполнения операций настройки, обновления, обслуживания компонентов Объекта Услуг. В данном режиме функции Объекта Услуг полностью или частично становятся недоступными для Пользователей. Технологические перерывы на выполнение плановых работ по обслуживанию должны быть согласованы с Заказчиком в части объема работ, состава работ и участников, времени начала и продолжительности работ.

3.3. Ограничения в части оказания Услуг

3.3.1. Услуги не включают работы по настройке, ремонту или замене каких-либо аппаратных компонентов Объектов Услуг.

3.3.2. Услуги не включают устранение последствий, возникших в результате:

- злонамеренных действий Заказчика или третьих лиц по отношению к Объектам Услуг;

- действий Заказчика или третьих лиц, если они были совершены вопреки эксплуатационной документации на Объект Услуг;
- проблем, относящихся к сторонним программным, аппаратным или инженерным компонентам, не входящим в состав Объектов Услуг;
- использования Заказчиком в составе Объектов Услуг аппаратных компонентов, не соответствующих требованиям к Объектам Услуг, установленным производителем программных компонентов Объектов Услуг для имеющегося количества пользователей;
- использования Заказчиком Объектов Услуг способом или в целях, для которых они не были предназначены;
- установки, перенастройки, модификации программных, аппаратных или инженерных компонентов Объектов Услуг без предварительного уведомления Исполнителя.

3.3.3. Услуги не включают обучение Пользователей работе с Объектами Услуг, а также не включают выдачу сертификатов, подтверждающих квалификацию Пользователей для работы с Объектами Услуг.

3.3.4. Услуги не включают участие специалистов Исполнителя в различного рода мероприятиях Заказчика, связанных с Объектами Услуг, например, в программах тестирования возможностей Объектов Услуг, в совещаниях, посвященных проектам внедрения смежных ИТ-решений Заказчика, если иное не указано в составе конкретной услуги. Все задачи, связанные с Услугами, подаются Заказчиком в виде заявок в Службу технической поддержки Исполнителя, в том числе и по вопросам взаимодействия Объектов Услуг со смежными ИТ-решениями Заказчика.

3.3.5. Исполнителю запрещено производить несанкционированные изменения текущей конфигурации компонентов Объектов Услуг (ниже уровня, входящего в зону охвата Услуг) и журналов регистрации системных событий Объектов Услуг.

3.3.6. В случае возникновения ситуаций, связанных с несанкционированным изменением сотрудниками Исполнителя Объектов Услуг и журналов регистрации системных событий Объектов Услуг, а также связанных с несанкционированным доступом к документам и объектам Объектов Услуг Заказчика, стоимость Услуг за отчетный период может быть сокращена на 3 (три) % за каждый подтвержденный случай.

3.4. Перечень Объектов Услуг

3.4.1. Общая информация, перечень, основные характеристики Объектов Услуг, а также перечень включенных в объем ТЗ услуг по каждому Объекту Услуг приведены в таблице «Перечень и основные характеристики Объектов Услуг».

Перечень и основные характеристики Объектов Услуг

№ п/п	Наименование Объекта услуг	Код Объекта Услуг	Назначение Объекта услуг	Размещение Объекта услуг	Класс критичности	Технологическое окно	Перечень услуг, включенных в объем ТЗ
1.	Автоматизированная система хранения данных	СХД	Система предназначена для хранения электронных образов различных документов в разрезах категорий	Центр обработки данных (ЦОД) Заказчика	К-4	22:00-02:00 МСК	Сопровождение автоматизированной системы хранения данных, в том числе: Услуга 1. Обеспечение работоспособности. Услуга 2. Поддержка Пользователей. Услуга 3. Администрирование.

3.5. Требования к численности и квалификации персонала Исполнителя

3.5.1. Уровень квалификации и количество персонала Исполнителя должны быть достаточными для успешного оказания Услуг.

3.5.2. Служба технической поддержки Исполнителя должна включать специалистов в соответствии с таблицей ниже.

Специалисты Службы технической поддержки

№ п/п	Должность	Роль	Категория	Количество, чел.
1.	Сервис-менеджер	Сервис-менеджер	К4	Не менее 1
2.	Разработчик	Разработчик	К4	Не менее 2
3.	Архитектор	Архитектор	К4	Не менее 1
4.	Старший консультант	Консультант ТП	К3	Не менее 1
5.	Инженер	Инженер ТП	К3	Не менее 2
6.	Тестирующий	Тестирующий	К3	Не менее 1
7.	Аналитик	Аналитик	К3	Не менее 1
8.	Консультант	Консультант ТП	К2	Не менее 2
9.	Младший консультант	Консультант ТП	К1	Не менее 1

3.5.3. Оказание Услуг Исполнителем должно соответствовать принятой у Заказчика сервисно-ресурсной модели управления ИТ:

Сервисно-ресурсная модель управления ИТ

1-я линия поддержки	САСП (регистрация, диспетчеризация)			Служба организации сервисной деятельности, выделенный сервис- менеджер Исполнителя
	Служба технической поддержки Исполнителя			
2-я линия поддержки	Группа поддержки ИТ-инфраструктуры Исполнителя	Группа поддержки ППО и Пользователей Исполнителя		
3-я линия поддержки	Производитель и СПО и оборудования	Служба эксплуатации ЦОД	Производители ППО, средств разработки	

4. Требования к видам обеспечения

4.1. Требование к документационному обеспечению

4.1.1. Обновление и доработка Объектов Услуг должны сопровождаться:

- передачей Исполнителем Заказчику обновленного пакета эксплуатационной документации, если обновление или доработка Объектов Услуг включает создание новых или изменение существующих прикладных функций, требующих соответствующих изменений в документации.

4.2. Требования к организационному обеспечению

4.2.1. Стороны до начала оказания Услуг обмениваются сведениями об ответственных за оказание Услуг лицах, их контактных телефонах и адресах электронной почты.

4.2.2. Взаимодействие Сторон должно быть организовано в соответствии с Порядком оказания услуг, приведённом в приложении 3 к настоящему ТЗ.

5. Требования к защите информации и информационной безопасности

5.1. Общие требования

5.1.1. Требования к защите информации и конфиденциальности, указанные в данном разделе ТЗ, дополняют требования, указанные в соответствующем разделе Договора. В случае противоречия требований данного раздела с положениями Договора, считать верными положения Договора.

5.1.2. Оказание Услуг должно выполняться в соответствии с правилами информационной безопасности (приложение 5 к настоящему ТЗ).

5.1.3. Исполнитель гарантирует конфиденциальность информации Заказчика, полученной в процессе оказания Услуг, в случае передачи информации, составляющей коммерческую тайну, Исполнитель обязуется подписать соответствующее соглашение по утверждённой у Заказчика форме.

5.1.4. Исполнитель обязан провести инструктаж работникам, привлекаемым к оказанию Услуг (в том числе удаленно) по соблюдению Правил информационной безопасности и режима конфиденциальности информации, установленных Заказчиком, и предоставить Заказчику расписки об ознакомлении работников с локальными нормативными актами Заказчика о защите конфиденциальной информации.

5.1.5. Любая информация о функционировании информационной инфраструктуры Заказчика, ставшая известной Исполнителю, не должна без разрешения или поручения Заказчика передаваться третьим лицам. При этом, информация, содержащаяся в заявках Заказчика в Службу технической поддержки Исполнителя, в случае если такие заявки входят в состав Услуг, может быть передана представителям производителя компонентов Объектов Услуг, если такие действия (передача информации) требуются для оказания Услуг.

5.1.6. Специалисты Исполнителя обязаны не препятствовать записи журналов событий, связанных с их вмешательством в работу Объектов Услуг.

5.1.7. В случае проведения расследования инцидентов ИБ Исполнитель должен обеспечить полное содействие всех задействованных в обслуживании Объектов Услуг специалистов, а также работников, имеющих отношение к инциденту, предоставить необходимые пояснения, в том числе при необходимости в письменном и официальном виде.

5.2. Требования к АРМ специалистов Исполнителя

5.2.1. АРМ специалистов Исполнителя, используемые для оказания Услуг (в том числе удаленно) должны соответствовать следующим требованиям:

- на АРМ должно быть установлено антивирусное ПО, включенное в реестр российского ПО, с ежедневно обновляемыми антивирусными базами;
- используемая ОС должна иметь установленные актуальные обновления безопасности;
- длина пароля учетной записи должна составлять, включая прописные буквы, цифры и специальные символы:
 - для Работников с правами «пользователя» не менее 15 символов;
 - для Работников с правами «администратора» (локального/доменного) не менее 20 символов;
 - для сервисных учетных записей не менее 20 символов;
 - для разделяемых ключей шифрования (shared keys) не менее 32 символов (256 бит);
- на АРМ не должно быть установленного ПО для организации удаленного доступа к информации или ОС (в т.ч. программ типа TeamViewer, RAdmin и т.п.);
- Не допускается указание услуг с использованием мобильных АРМ или общедоступных АРМ;
- По окончании сеанса работы на АРМ или при необходимости оставления рабочего места Работник должен заблокировать экран средств вычислительной техники (блокирование экрана на персональном компьютере осуществляется нажатием сочетания клавиш Win + L или нажатием сочетания клавиш Ctrl + Alt + Del и выбором опции «Блокировать компьютер»).

6. Перечень и порядок оказания Услуг

6.1. Требования к составу и содержанию Услуг

6.1.1. Состав и содержание Услуг приведены в приложении 1 к настоящему ТЗ.

6.2. Порядок оказания Услуг

6.2.1. Порядок оказания Услуг приведён в приложении 3 к настоящему ТЗ.

6.2.2. Исполнитель в соответствии с указанным в карточках Услуг (см. приложение 1) графиком активирования осуществляет подготовку, согласование и предоставление Заказчику бухгалтерских и отчётных документов.

6.2.3. Формы отчётных документов приведены в приложении 4 к настоящему ТЗ.

7. Перечень приложений

Приложение 1. Перечень и содержание Услуг;

Приложение 2. Перечень передаваемых документов;

Приложение 3. Порядок оказания Услуг;

Приложение 4. Формы отчётных документов;

Приложение 5. Правила информационной безопасности.

ЗАКАЗЧИК:

АО «Россети ЦИУС ЕЭС»

ИСПОЛНИТЕЛЬ:

_____/_____/

_____/_____/

Приложение 1
к Техническому
заданию

1

Приложение 1. Перечень и содержание Услуг

1. Объект Услуг: Автоматизированная система хранения данных (СХД).

1.1. Компонентный состав

1.1.1. Объект Услуг включает следующие программные, аппаратные, инженерные и иные компоненты:

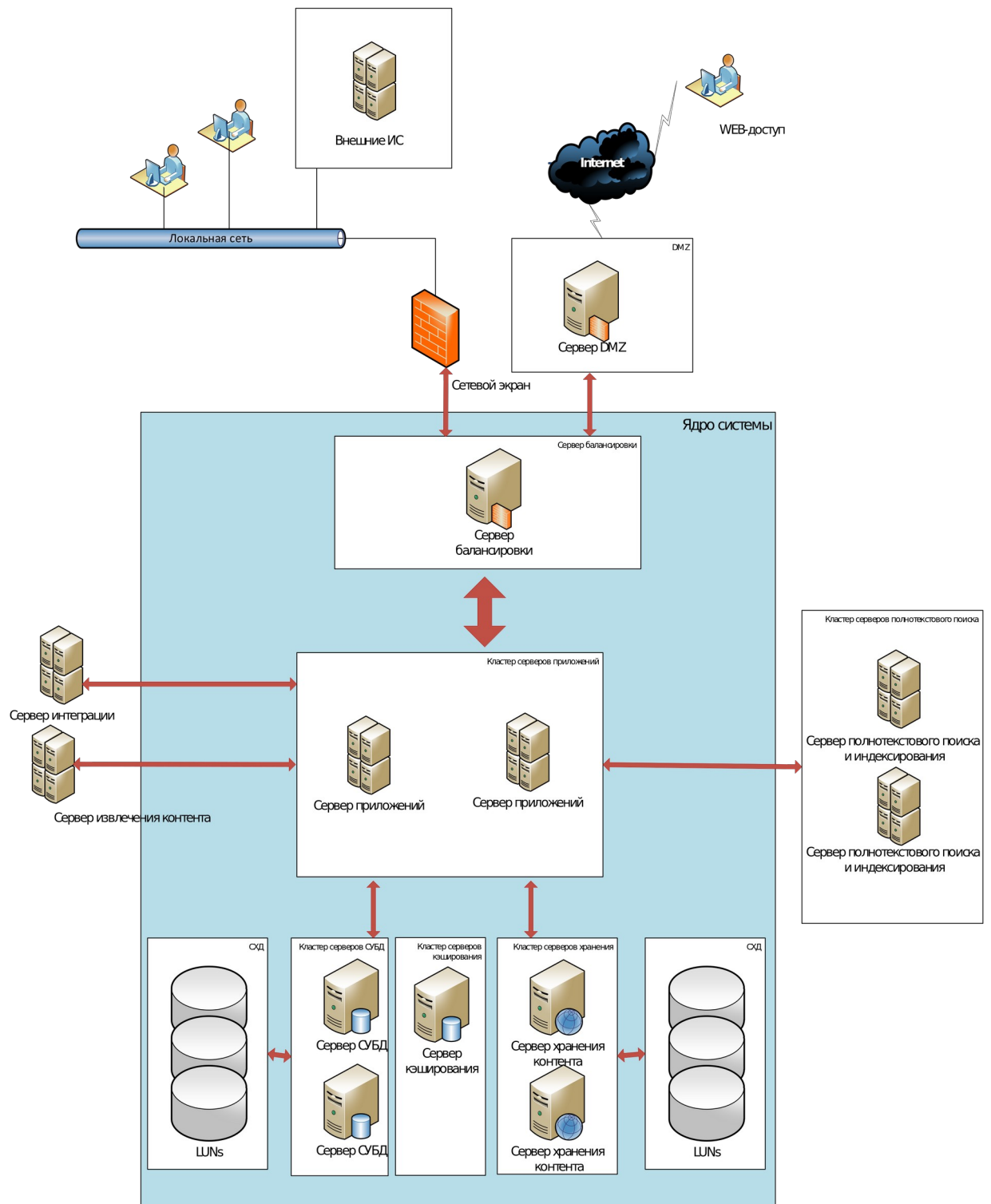
Компоненты

№ п/п	Наименование компонента Объекта Услуг	Категория компонента Объекта Услуг
1.	Модуль «Хранение документов»	Прикладное ПО
2.	Модуль «Ввод»	Прикладное ПО
3.	Модуль «Вывод»	Прикладное ПО
4.	Модуль «Безопасность»	Прикладное ПО
5.	Модуль «Администрирование»	Прикладное ПО
6.	Модуль «Навигация, поиск, фильтрация, сортировка и просмотр»	Прикладное ПО
7.	Модуль «Статистическая отчетность»	Прикладное ПО
8.	Модуль «Интеграция с 1С ЗУП»	Интеграционные механизмы
9.	Модуль «Интеграция с СЭДО»	Интеграционные механизмы
10.	Модуль «Интеграция с СЭА»	Интеграционные механизмы
11.	Модуль «Интеграция с КИСУ ЦИУС»	Интеграционные механизмы
12.	Сервер СУБД PostgreSQL/Postgres PRO 11 2 шт – продуктивная среда 1 шт – тестовый контур	Системное ПО
13.	Сервер балансировки Nginx 1 шт	Системное ПО
14.	Сервер кэширования	Системное ПО

	MongoDB 1 шт	
15.	Серверы приложений Java 11.x Tomcat server 9.x. Nginx 1.22.x 2 шт – продуктивная среда 1 шт – тестовый контур	Системное ПО
16.	Сервер хранения контента Java, IO Server, Tomcat 2 шт	Системное ПО
17.	Сервер поиска Java, ElasticSearch 2 шт	Системное ПО
18.	Сервер интеграции Java 11.x Tomcat server 9.x. Nginx 1.22.x 1 шт	Системное ПО
19.	Сервер извлечения контента Java, Tika, Nginx 1 шт	Системное ПО

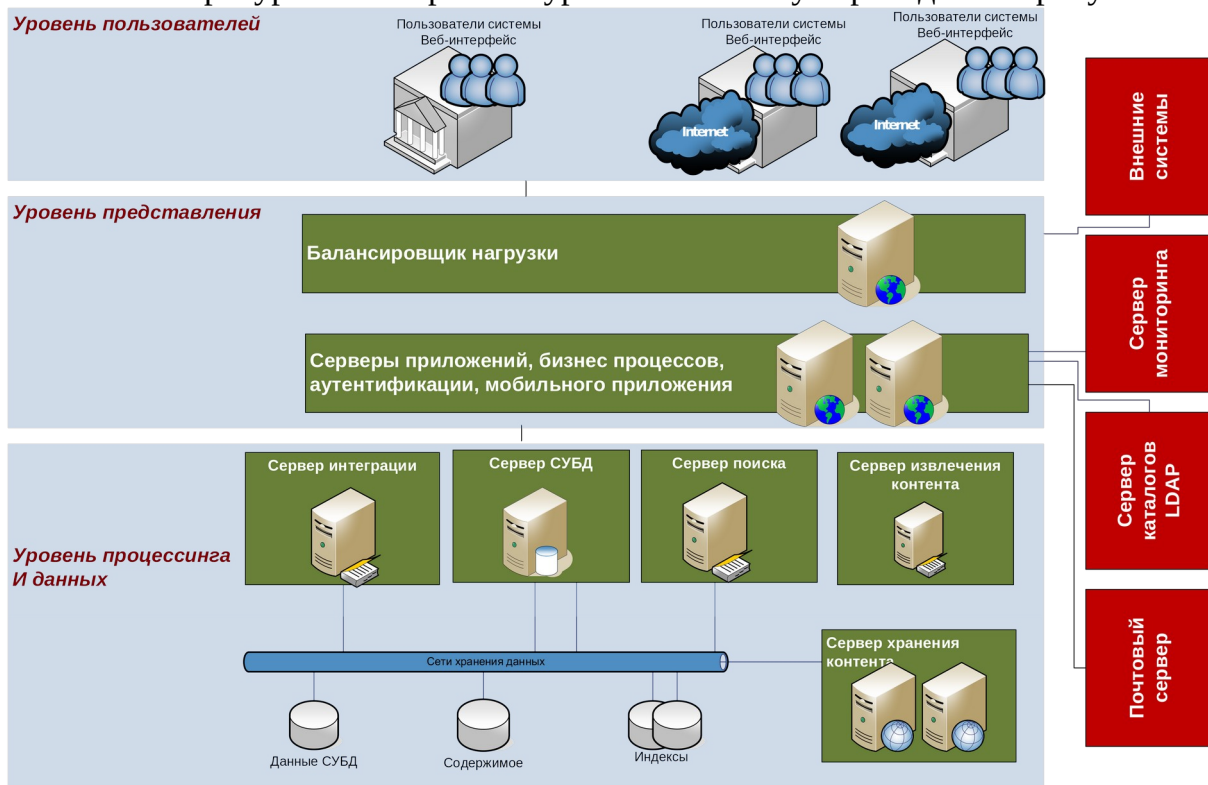
1.1.2. Перечень компонентов Объекта Услуг в разрезе категорий, в отношении которых оказываются Услуги сопровождения по настоящему ТЗ, приведен в следующем разделе «Зона охвата Услуг».

1.1.3. Структурная схема Объекта Услуг приведена на рисунке ниже:



Структурная схема

1.1.4. Трехуровневая архитектура Объекта Услуг приведена на рисунке ниже:



трехуровневая архитектура

Тр

1.2. Зона охвата Услуг

1.2.1. Категории компонентов Объекта Услуг, в отношении которых оказываются Услуги в соответствии с настоящим ТЗ:

Зона охвата Услуг

№ п/п	Категория компонента Объекта Услуг	Входит в зону охвата Услуг
1.	Прикладное ПО	ДА
2.	Интеграционные механизмы	ДА
3.	Системное ПО (серверные операционные системы, СУБД, прочие утилиты)	ДА
4.	Виртуальная ИВИ	НЕТ
5.	Аппаратная ИВИ	НЕТ
6.	Прочее оборудование	НЕТ
7.	Инженерные системы	НЕТ

1.2.2. Категории компонентов, которые не входят в объем Услуг, обслуживаются на стороне Заказчика и/или иных исполнителей.

1.3. Карточки Услуг

Услуга 1. Обеспечение работоспособности

№ п/п	Название	Описание
1.	Код Услуги	БИЗ.ИС.СХД-01.
2.	Название Услуги	Комплекс мероприятий по обеспечению бесперебойного функционирования Объекта Услуг.
3.	Категория Услуги	Бизнес-услуга.
4.	Функциональный заказчик	См. п. 3.4.
5.	Перечень работ в составе Услуги	Выполнение заявок Заказчика; - нахождение временных решений до момента решения сбоев; - устранение нарушений работоспособности Объекта Услуг; - устранение ошибок со входом в систему; - устранение ошибок при выявлении расхождения функционала с документацией; - устранение ошибок при выявлении сбоев отображения экранных форм; - устранение ошибок при выявлении ошибок в отображаемых данных; - поддержка работоспособности сопровождаемой системы в объеме функций интеграционных сервисов в соответствии с Регламентом обработки обращений Пользователей, связанных с интеграцией (Приложение 1.1. к Техническому заданию); - анализ производительности и формирование предложений по оптимизации и развитию системно-технического комплекса; - контроль доступности и функционирования Объекта Услуг на уровне операционных систем, прикладных систем; - устранение ошибок работы подсистемы журналирования Объекта Услуг; - мониторинг корректности формирования журналов,

		организация ротации журналов и оптимального архивного хранения журналов; - мониторинг ресурсов и показателей производительности вычислительного комплекса на уровне операционных систем и прикладного ПО; - мониторинг доступности и показателей функционирования Объекта Услуги, его модулей и подсистем, включая интеграционные сервисы; - мониторинг файловых систем и СУБД; - самостоятельная инициация выполнения услуг обеспечения работоспособности Объекта Услуг при обнаружении отклонений, влияющих на работоспособность Объекта Услуг по данным мониторинга, не дожидаясь заявок Пользователей. В том числе при обнаружении тенденций ведущих к сбою Объекта Услуг в текущем или следующем отчётном периоде. Такие заявки не являются фиктивными. - изменение настроек программно-аппаратного комплекса (по мере необходимости); - изменение настроек программных компонентов Системы (по мере необходимости);
6.	График активирования	<i>Ежемесячно.</i>
7.	Режим оказания Услуги	<i>Рабочее время.</i>
8.	Соглашение об уровне Услуги	Целевая доступность Объекта Услуг: 98 %. Время реакции: 30 мин. Время решения: - Критические заявки - 8 ч; - Важные заявки - 28 ч; - Обычные заявки - 56 ч. Время решения может быть изменено (увеличено или уменьшено) по согласованию Сторон. Целевое исполнение заявок в срок в отчётном периоде - не менее 95 %. Целевое количество фиктивных заявок - не более 1 шт. Целевое количество опротестованных заявок - не более 5 % от общего числа поступивших заявок в отчётный период.

9.	Объём Услуги	Количество конфигурационных единиц – см. п.4.1.1.
10.	Зона охвата Услуги	См. раздел «Зона охвата Услуг» для данного Объекта Услуг.
11.	Порядок оказания Услуги	В соответствии с приложением 3 к настоящему ТЗ.
12.	Штрафные санкции	5 % от стоимости Услуги «Обеспечение работоспособности» в отчётном периоде: - исполнение заявок в срок менее целевого более 5% до 10% включительно; - ИЛИ - количество фиктивных заявок более 1 шт.; - ИЛИ - количество опротестованных заявок более 5% - ИЛИ - доступность ниже целевой (отклонение до 0,2%). 10 % от стоимости услуги «Обеспечение работоспособности» в отчётном периоде: - исполнение заявок в срок менее целевого - более 10% - ИЛИ - доступность значительно ниже целевой (отклонение более чем на 0,2%). Максимальный штраф по Услуге - не более 15 % от стоимости Услуги «Обеспечение работоспособности» в отчётном периоде.

-
1. В случае если исправления ошибки или доработки потребовали обе системы, а также в случае отказа в доработке (п.6) ответ на обращение пользователя осуществляет Служба технической поддержки СХД.
 2. Любая доработка одной или обеих систем, затрагивающая функционал интеграции, перед переносом на продуктивные площадки должна пройти совместное тестирование на площадках аналогичных продуктивным.
 3. Любые переносы запросов в продуктивную систему Службой технической поддержки СХД или службой технической поддержки смежной системы должны быть согласованы с функциональным Заказчиком. Для этого требуется направить письмо по электронной почте в адрес ответственного лица от Заказчика с уведомлением Службы технической поддержки СХД или службы технической поддержки смежной системы. В письме требуется указать номера запросов на перенос и краткое описание содержания запроса. Ответственное лицо от Заказчика в течение суток согласуют возможность переноса изменений, инициируя при этом резервное копирование системы на текущую дату.
 4. Запрос с изменением функциональности может быть перенесен в продуктивную систему только после получения согласования ответственного лица от Заказчика и информации о том, что резервное копирование системы проведено.

Услуга 2. Поддержка Пользователей

№ п/ п	Название	Описание
1.	Код Услуги	БИЗ.ИС.СХД-02.
2.	Название Услуги	Комплекс мероприятий по информационно-техническому сопровождению Пользователей в части оказания консультаций и предоставлению документации по работе с Объектом Услуги.
3.	Категория Услуги	Бизнес-услуга.
4.	Функциональный заказчик	См. п. 3.4.
5.	Перечень работ в составе Услуги	- Выполнение заявок Пользователей; - анализ заявок и оказание консультаций Пользователям по возможностям, использованию функций и режимам функционирования Объекта Услуг; - решение вопросов пользователей; - разъяснение инструкций; - консультации по выполнению действий в Объекте услуг; - методологическая поддержка пользователей по работе с функционалом Объекта Услуг; - консультация по ограничениям функционала Объекта Услуг; - консультация пользователей по организационным вопросам при работе в Объекте Услуг в рамках основных бизнес-процессов, реализованных и переданных в промышленную эксплуатацию; - решение вопросов, требующих выполнения настроек рабочих мест пользователей; - консультирование по вопросам интеграции с другими информационными системами на стороне Объекта Услуг; - проведение очного консультирования пользователей по работе в Объекте Услуг.
6.	График активирования	<i>Ежемесячно.</i>
7.	Режим оказания Услуги	<i>Рабочее время.</i>

8.	Соглашение об уровне Услуги	Время реакции: 30 мин. Время решения: - Критические заявки - 8 ч; - Важные заявки - 24 ч; - Обычные заявки - 56 ч. Время решения может быть изменено (увеличено или уменьшено) по согласованию Сторон. Целевое исполнение заявок в срок в отчётном периоде - не менее 95 %. Целевое количество фиктивных заявок - не более 1 шт. Целевое количество опротестованных заявок - не более 5 % от общего числа поступивших заявок в отчётный период.
9.	Объём Услуги	Количество Пользователей - не более 1500 чел.
10.	Зона охвата Услуги	См. раздел «Зона охвата Услуг» для данного Объекта Услуг.
11.	Порядок оказания Услуги	В соответствии с приложением 3 к настоящему ТЗ.
12.	Штрафные санкции	5 % от стоимости Услуги «Поддержка Пользователей» в отчётном периоде за: - исполнение заявок в срок менее целевого – от 6% до 10%; ИЛИ - количество фиктивных заявок более 1 шт.; ИЛИ - количество опротестованных заявок более 5% от общего количества заявок в отчетном периоде. 10 % от стоимости Услуги «Поддержка Пользователей» в отчётном периоде за: - исполнение заявок в срок менее целевого - более 10%. Максимальный штраф - не более 10 % от стоимости Услуги «Поддержка Пользователей» в отчётном периоде.

Услуга 3. Администрирование

№	Название	Описание
п/п		

1.	Код Услуги	БИЗ.ИС.СХД-03.
2.	Название Услуги	Комплекс мероприятий по администрированию Объекта Услуг.
3.	Категория Услуги	Бизнес-услуга.
4.	Функциональный заказчик	См. п. 3.4.
5.	Перечень работ в составе Услуги	- Выполнение заявок Пользователей; - заведение новых учётных записей Пользователей, настройка прав доступа и/или зон видимости в соответствии с реализованными ролями и полномочиями Объекта Услуг; - удаление и/или блокировка учётных записей Пользователей; - изменение прав доступа и/или зон видимости Пользователей к функциональности Объекта Услуг; - настройка режимов работы компонентов Объекта Услуг; - восстановление данных и компонентов Объекта Услуг из резервных копий; - выполнение необходимых мероприятий по настройке функционирования Объекта Услуг; - управление контентом в соответствии с регламентами, администрирование параметров системы, связанных с контентом; - администрирование журналов операций с документами Объекта Услуг; - управление доступностью модулей; - исправление прикладных ошибок в работе пользователей Объекта Услуг; - анализ системных журналов и файловых систем на наличие ошибок, поиск и применение решений по их исправлению; - проведение работ, выполняемых вручную администраторами для устранения последствий функциональных ошибок и сбоев в период, пока ошибки и иные причины сбоев не устранены обновлениями системы; - настройка параметров интеграции с КИСУ ЦИУС по результатам ввода интеграции в промышленную

		эксплуатацию, а также при создании новых классов, подлежащих интеграции с КИСУ ЦИУС; - выполнение регламентных работ, предусмотренных эксплуатационной документацией; - восстановление системы из резервных копий (совместно с представителем Заказчика, эксплуатирующим систему резервного копирования и восстановления); - восстановление зоны эксплуатации Объекта Услуг после чрезвычайных и аварийных ситуаций, включая восстановление резервирования подсистем согласно проектному решению; - запуск, останов, перезагрузка серверов Объекта Услуг.
6.	График активирования	<i>Ежемесячно.</i>
7.	Режим оказания Услуги	<i>Рабочее время.</i>
8.	Соглашение об уровне Услуги	Время реакции: 30 мин. Время решения: - Критические заявки - 8 ч; - Важные заявки - 24 ч; - Обычные заявки – 48 ч. Время решения может быть изменено (увеличено или уменьшено) по согласованию Сторон. Целевое исполнение заявок в срок в отчётном периоде - не менее 95 %. Целевое количество фиктивных заявок - не более 1 шт. Целевое количество опротестованных заявок - не более 5 % от общего числа поступивших заявок в отчётный период.
9.	Объём Услуги	Количество конфигурационных единиц - см. п.4.1.1. Количество Пользователей - не более 1500 человек.
10.	Зона охвата Услуги	См. раздел «Зона охвата Услуг» для данного Объекта Услуг.
11.	Порядок оказания Услуги	В соответствии с приложением 3 к настоящему ТЗ.
12.	Штрафные санкции	5 % от стоимости Услуги в отчётном периоде за: - исполнение заявок в срок менее целевого – от 6% до 10%; ИЛИ

		- количество фиктивных заявок более 1 шт.; ИЛИ - количество опротестованных заявок более 5% 10 % от стоимости услуги в отчётном периоде: - исполнение заявок в срок менее целевого - более 10%. Максимальный штраф - не более 10 % от стоимости Услуги в отчётном периоде.
--	--	--

ЗАКАЗЧИК:
АО «Россети ЦИУС ЕЭС»

ИСПОЛНИТЕЛЬ:

_____ / _____ /

_____ / _____ /

**Регламент обработки обращений Пользователей,
связанных с интеграцией СХД**

1. Интеграция осуществляется в соответствии с актуальными версиями документов, регламентирующими техническое взаимодействие различных систем (субсистем) и СХД. В случае внесения изменений в такие документы и/или принятия новых данных Регламент не изменяется.
2. При поступлении обращения Пользователя по инциденту, связанному с Интеграцией, Служба технической поддержки проводит диагностику проблемы и в случае если проблема на стороне СХД, пользователю направляется ответ с решением.
3. В случае если проблема на стороне смежной системы, Служба технической поддержки СХД направляет соответствующее обращение в службу технической поддержки смежной системы. Обращение приобретает статус с пометкой «Передано в ... (СП КИСУ ЦИУС или СЭА или СЭДО или 1С ЗУП)». После решения проблемы ответ пользователю направляет служба технической поддержки, осуществлявшая решение инцидента. Копия ответа направляется службе технической поддержки смежной системы (принявшей обращение). Поддержка первой стороны не может закрыть обращение, без закрытия обращения второй.
4. В случае если проблема требует доработки одной или обеих систем, данная информация направляется ответственному лицу от Заказчика. В этом случае принимается совместное решение о необходимости доработки.
5. В случае если доработка незначительна и возможна в рамках настоящего договора поддержки, см. пп. 2 и 3.
6. В случае если доработка требует существенных трудозатрат, она заносится в Реестр нерешенных инцидентов Заказчика. Пользователю направляется ответ.

№ п/п	Описание проблемы	Принято Службой поддержки (наименование)	Дата и время обращения	Пользователь (ФИО, e-mail/телефон)	Комментарий поддержки 1	Комментарий поддержки 2	Комментарий Заказчика
1	2	3	4	5	6	7	8

Статус	Дата и время закрытия обращения
9	10

1. **№ п/п** - нумерация сквозная
2. **Описание проблемы** - копия текста обращения пользователя по электронной почте или стенограмма телефонного обращения
3. **Принято Службой технической поддержки** – СХД или смежная система, дата
4. **Дата обращения** - в формате ДД.ММ.ГГГГ
5. **Пользователь (ФИО, e-mail/телефон)** - ФИО - полностью, телефон - в формате «(код) номер доб. номер». Например, Иванов Иван Иванович, Ivanov I@sius-ees.ru или Петрова Мария Петровна (4212) 11-22-33 доб. 4455
- 6,7,8. Комментарии участников процесса.

Форма согласована

ЗАКАЗЧИК

ИСПОЛНИТЕЛЬ

_____/_____/

М.П.

_____/_____/

М.П.

Приложение 2
к Техническому
заданию

2 Приложение 2. Перечень передаваемых документов

№ п/п	Наименование документа	Формат документа
1.	Руководство пользователя	электронный pdf
2.	Руководство администратора	электронный pdf
3.	Описание системного и интеграционного ландшафта	электронный pdf
4.	Проектное решение	электронный pdf

ЗАКАЗЧИК:
АО «Россети ЦИУС ЕЭС»

ИСПОЛНИТЕЛЬ:

_____/_____/

_____/_____/

3 Приложение 3. Порядок оказания Услуг

1. Общие положения

1.1. В настоящем документе (далее – Порядок) представлено описание порядка взаимодействия между сотрудниками Заказчика и сотрудниками Исполнителя в рамках оказания Услуг. Настоящий документ является неотъемлемым приложением к ТЗ.

1.2. В целях удобства понимания Порядка, под термином Заказчик понимается как организация Заказчика, так и пользователи Объекта Услуг Заказчика. Под термином Исполнитель понимается как организация Исполнителя, так и сотрудники Исполнителя, привлекаемые им для оказания Услуг.

1.3. Язык взаимодействия со Службой технической поддержки Исполнителя в том числе с использованием САСП – русский.

2. Термины, определения и сокращения

2.1. Термины, сокращения и определения приведены в соответствующем разделе ТЗ.

3. Обязанности Исполнителя

3.1. Исполнитель принимает и обрабатывает заявки Заказчика в целях оказания Услуг в соответствии с ТЗ.

3.2. Исполнитель использует для оказания Услуг САСП Исполнителя. Поддержка работоспособности САСП осуществляется силами и за счёт Исполнителя.

3.3. Исполнитель обрабатывает поступающие заявки Пользователей в САСП в соответствии с п.6 настоящего Порядка.

3.4. Исполнитель осуществляет работы только по заявкам, если иное не указано в описании Услуг.

3.5. Исполнитель согласует с Заказчиком проведение работ по обслуживанию программных, аппаратных и инженерных компонентов Объектов Услуг, требующих полную или частичную их остановку.

3.6. В случае привлечения Исполнителем к оказанию Услуг третьих лиц (других подрядных организаций), Исполнитель несет ответственность за их действия как за свои собственные.

3.7. Исполнитель несет ответственность за качественное оказание Услуг в соответствии с Соглашением.

4. Обязанности Заказчика

4.1. САСП регистрирует заявки пользователей и обеспечивает направление заявок на в поддержку Исполнителя.

4.2. Заказчик по запросу Исполнителя обеспечивает предоставление Исполнителю всей необходимой информации и документации для оказания Услуг.

4.3. Заказчик при обращении в Службу технической поддержки Исполнителя руководствуется следующим принципом: направляемая в САСП заявка должна содержать вопрос или проблему, которые Исполнитель может решить в рамках одной Услуги. Если у Заказчика есть потребность в решении нескольких вопросов, соответствующих разным услугам или одной, но с разной критичностью, то Заказчик должен направить данные вопросы отдельными заявками.

5. Ответственные лица

5.1. Для определения порядка взаимодействия, а также для распределения ответственности за полученный результат со стороны Заказчика и Исполнителя назначаются ответственные лица в соответствии с таблицей ниже (заполняется в процессе заключения Договора).

Роль	Краткое описание	Ф.И.О. и контакты
Менеджер по контролю качества оказания услуг	Со стороны Заказчика. Осуществляет контроль качества предоставления Услуг	<...>
Сервис-Менеджер	Со стороны Исполнителя. Отвечает за решение вопросов, связанных с организацией предоставления Услуг	<...>
Основной инженер	Со стороны Исполнителя. Отвечает за решение вопросов, связанных с непосредственным оказанием Услуг	<...>

6. Обработка заявок

6.1. Общие положения

6.1.1. В настоящем Разделе приводятся основные принципы обработки заявок.

6.1.2. Основанием для выполнения работ Исполнителем является заявка, зарегистрированная в САСП.

6.1.3. Исполнитель обеспечивает следующую последовательность обработки заявки:

- после получения заявки на свою линию исполнения уточняет информацию по заявке (Объект Услуг, его компонент, услуга, прочая информация) и вносит ее в САСП;
- после уточнения данных по заявке назначает заявке приоритет и приступает к ее решению;
- обеспечивает решение заявок, зарегистрированных в САСП в установленные сроки в соответствии с требованиями, указанными в карточке Услуг;
- вносит в САСП информацию о состоянии решения заявок;
- при необходимости запрашивает дополнительную информацию у Заказчика, необходимую для решения заявки;
- осуществляет мониторинг исполнения заявок и соответствующую эскалацию: в случае задержек на стороне Заказчика – на Менеджера по контролю качества оказания услуг, в случае задержек на стороне третьих лиц – на контактные данные Сервис-Менеджера третьих лиц, в случае задержек на стороне Исполнителя – на руководство Исполнителя;
- при необходимости привлечения специалистов Заказчика и/или других подрядных организаций Исполнитель самостоятельно контактирует с ними и осуществляет общую координацию действий при исполнении заявки;
- информирует Заказчика о статусе и ходе работ по заявке по запросу;
- обеспечивает информативное оперативное отражение хода работ в САСП.

6.2. Регистрация, классификация и назначение обращения

6.2.1. Подача заявки осуществляется посредством отправки Заказчиком сообщения (заявки) по электронной почте на адрес САСП или созданием заявки непосредственно в САСП.

6.2.2. Полученные заявки регистрируются в САСП.

6.2.3. Номер и дата регистрации заявки направляется письмом по электронной почте Заказчику автоматически из САСП.

6.2.4. Заявка может относиться к любой из указанных ниже категорий:

- Инцидент (сбой);
- ЗНО.

6.2.5. В случае нарушения сотрудником Заказчика принципа формирования заявки в САСП, описанного в п. 4.3 настоящего Порядка, специалист САСП вправе отклонить некорректно составленную заявку, указав в комментарии рекомендации по разнесению комплекса вопросов по отдельным заявкам.

6.2.6. Заявка должна содержать следующую обязательную информацию:

- ФИО пользователя, организация пользователя, адрес электронной почты пользователя и его контактный телефон;
- тема (наименование Объекта Услуг, по которому создается обращение, краткое изложение описания запроса);
- подробное описание заявки:
 - для сбоев:
 - фактический результат функционирования,

- ожидаемый результат функционирования,
 - указание на способ воспроизведения,
 - текст ошибки при наличии,
 - учётная запись, под которой получена ошибка;
- о для ЗНО:
- описание подробного запроса.

6.2.7. К содержимому заявки могут быть приложены дополнительные материалы, которые могут быть полезны Исполнителю:

- скриншот (снимок с экрана), форматы файлов: jpg, png;
- текстовые и табличные документы с развернутым и / или наглядным описанием заявки;
- видеозапись, фиксирующая действия Пользователя, приводящие к ошибке.

6.2.8. Для каждой заявки Исполнитель указывает значения приоритета в соответствии с приведённой ниже таблицей:

Приоритет	Описание проблемы и влияние на бизнес
Критический	Критическое влияние на бизнес: Дальнейшая работа с функционалом Объекта Услуг невозможна. Объект Услуг не выполняет требуемые функции. Заказчик не может решить проблему самостоятельно. Проблемы данного уровня: - зависание или масштабный сбой Объекта Услуг; - повреждение данных Объекта Услуг; - недоступность критически важного функционала Объекта Услуг.
Высокий	Значительное влияние на бизнес: Логика работы функционала Объекта Услуг серьёзно нарушена. Существует обходное решение, но оно не очевидно для Заказчика, либо невозможно без специальных средств. Проблемы данного уровня: - значительный сбой Объекта Услуг.
Обычный	Формальное влияние на бизнес: Незначительные проблемы, которые не влияют на функционирование Объекта Услуг и работу Заказчика. Проблемы данного уровня: - незначительный сбой Объекта Услуг; - запрос на обслуживание.

6.2.9. В случае несоответствия назначенного Исполнителем приоритета (согласно таблице выше), САСП вправе изменить приоритет заявки по требованию Менеджера по контролю качества Заказчика. Изменение приоритета сопровождается уведомлением Исполнителя.

6.3. Диагностика и решение заявки

6.3.1. После направления заявки на исполнение Исполнитель обязан:

- принять заявку в работу;
- провести первичный анализ;
- внести информацию о результатах анализа и планируемых мерах по исполнению заявки в САСП.

6.3.2. Исполнитель выполняет работы по заявке и вносит в САСП подробную информацию о ходе работ и полученном результате.

6.3.3. Исполнитель имеет право запросить у Заказчика дополнительную информацию, обоснованно необходимую для анализа и выработки методов решения заявки. При этом работы по анализу заявки могут быть приостановлены до момента получения запрошенной информации от Заказчика.

6.3.4. Время ожидания дополнительной информации не учитывается при подсчете времени исполнения заявки.

6.3.5. Если в течение **<5 (пяти)>** рабочих дней с момента отправки Исполнителем запроса на предоставление уточняющих данных по заявке ответа от Заказчика не поступило, то такая заявка снимается с исполнения (отклоняется). При отклонении заявки Исполнитель добавляет обоснованный комментарий о невозможности обработки заявки, т.к. по ней не была представлена вся необходимая информация.

6.3.6. Исполнитель может предложить Пользователю временное решение, в случае если постоянное решение требует большее время реализации.

6.3.7. В случае если для решения заявки необходимо внесение изменений в СХД в т.ч. в справочники, классы и т.д. Исполнитель согласовывает данные изменения с ответственными лицами Заказчика.

6.3.8. В случае если для решения заявки необходимо участие Заказчика или его подрядных организаций (например, для физической перезагрузки сервера, восстановления БД из резервной копии и т.д.), Исполнитель самостоятельно организует и координирует такие работы. Время исполнения заявки на стороне Заказчика и его подрядных организаций не учитывается при подсчете времени исполнения заявки.

6.3.9. Если в случае поступления заявки Исполнитель выясняет, что причиной возникновения описанной в ней проблемы является инфраструктурный инцидент на стороне Заказчика (незапланированная остановка работы аппаратного комплекса, снижение производительности или функциональности, т.е. сбой или отказ аппаратного ПО, а также в случае, если ошибка связана с функционированием системного либо базисного ПО), Исполнитель уведомляет об этом Менеджера по контролю качества оказания услуг Заказчика, делает соответствующий комментарий, после окончания работ на стороне Заказчика – проверяет работу Объекта Услуг и закрывает заявку. Время исполнения заявки

на стороне Заказчика и его подрядных организаций не учитывается при подсчете времени исполнения заявки.

6.3.10. Если с целью исполнения заявки Исполнителем установлена необходимость выполнения дополнительных работ, входящих в состав другой Услуги, ему необходимо проинформировать Заказчика и организовать получение от него новой заявки.

6.4. Закрытие заявок

6.4.1. После завершения работ по заявке Исполнитель вносит соответствующую информацию в САСП и переводит заявку в статус завершения работ.

6.4.2. Заказчик, получив уведомление о завершении работ по заявке, должен выполнить проверку результата выполнения работ по заявке. Если результат устраивает Заказчика, то он принимает работы по заявке. В противном случае он отклоняет работы по заявке.

6.4.3. Если работы отклонены, и заявка возвращена на исполнение, то такая заявка считается опротестованной и исполнение работ по ней начинается заново.

6.4.4. Срок работ по опротестованной заявке согласуется Сторонами в рабочем порядке.

6.4.5. Заявка, выполнение которой согласовано или результаты работ приняты, считается выполненной и закрытой.

6.4.6. Если Пользователь, направивший заявку, не принял и не отклонил работы по заявке, то по истечению 10 (десяти) рабочих дней Заявка считается закрытой.

6.4.7. Срок исполнения заявок рассчитывается как разность между временем получения Исполнителем заявки на исполнение и временем последнего перевода заявки Исполнителем в статус завершения работ, исключая время, на которое работы по выполнению заявки были приостановлены (запрос уточняющей информации или ожидание устранения Заказчиком проблем, препятствующих выполнению заявки)

7. Проведение плановых и аварийных работ

7.1. Проведение плановых работ, связанных с полной или частичной недоступностью функций Объекта Услуг (например, для обновления компонентов Объекта Услуг).

7.1.1. Плановые работы проводятся в период технологического окна или во временной интервал, согласованный Сторонами.

7.1.2. Не менее чем за 1 (один) рабочий день до начала проведения плановых работ Исполнитель обязан уведомить Менеджера по контролю качества оказания услуг Заказчика и организовать соответствующее уведомление всех заинтересованных в функционировании Объекта Услуг лиц посредством службы САСП.

7.2. Проведение внеплановых (аварийных) работ, связанных с устранением сбоев в работе Объекта Услуг.

7.2.1. В случае необходимости проведения аварийных работ для устранения сбоев в работе Объекта Услуг Исполнитель имеет право инициировать и согласовать с Заказчиком проведение внеплановых работ. Для этого Исполнитель обязан незамедлительно уведомить Менеджера по контролю качества оказания услуг Заказчика и организовать соответствующее уведомление всех заинтересованных в функционировании Объекта Услуг лиц посредством службы САСП.

7.3 Общие сведения для проведения плановых и аварийных работ.

7.3.1. Типовой текст уведомления.

Уважаемые коллеги!

В рамках оказания услуг сопровождения <Информационной системы> будут проводиться <указываются необходимые работы>.

Плановое время начала работ - ЧЧ:ММ.

Плановое время окончания работ - ЧЧ:ММ.

В указанный период «<Информационная система> будет недоступна» / «будет недоступна ... функциональность <Информационной системы>».

С уважением, Единая Служба Поддержки Пользователей.

7.3.2. Заказчик имеет право перенести время выполнения плановых или аварийных работ, а также отказать Исполнителю в их выполнении.

7.3.4. Исполнитель не несет ответственности за функционирование Объекта Услуг в случае, если Заказчик отменил или перенес плановые или аварийные работы, если от них зависит функционирование Объекта Услуг.

ЗАКАЗЧИК:
АО «Россети ЦИУС ЕЭС»

ИСПОЛНИТЕЛЬ:

_____/_____/_____

_____/_____/_____

4 Приложение 4. Формы отчётных документов

Форма 1. Сводный отчёт по объёму оказанных Услуг

за период с ____ по ____

Отчет должен формироваться на основании данных САСП.

№ п/ п	Наименование ИС	Наименование Услуги	Объём оказанных Услуг, шт.	*Объём Услуг с отклонением от уровня оказания Услуг, шт.	**Штрафные санкции по Услуге, %
1					
2					

** Подсчитывается на основании Детального отчета по заявкам.*

*** Определяется на основании Соглашений об уровне оказания услуг для каждой Услуги (нарушение исполнения заявок, снижение доступности, ИБ-инциденты).*

от ЗАКАЗЧИКА

_____/_____/

.

от ИСПОЛНИТЕЛЯ

_____/_____/

Форма 2. Детальный отчёт по заявкам Пользователей за период с ____ по ____

Отчет должен формироваться на основании данных САСП.

Отчет предоставляется в электронном виде (в формате электронной таблицы).

№ п/п	Номер заявки	Тема заявки	Инициатор заявки	Наименование ИС	Услуга	Дата и время регистрации	Дата и время назначения на Исполнителя	Дата и время решения	*Нарушение Соглашения
1									ДА / НЕТ
2									ДА / НЕТ

* Указывается на основании Соглашений об уровне оказания услуг для каждой Услуги (нарушение сроков, опротестованные заявки, фиктивные).

от ЗАКАЗЧИКА

_____/_____/____.

от ИСПОЛНИТЕЛЯ

_____/_____/____.

Формы согласованы

ЗАКАЗЧИК

_____/_____/____.

М.П.

ИСПОЛНИТЕЛЬ

_____/_____/____.

М.П.

5 Приложение 5. Правила информационной безопасности

Введение

Целью разработки настоящих Правил информационной безопасности в АО «Россети ЦИУС ЕЭС» (далее – Правила) является определение правил работы с информацией конфиденциального характера, правил безопасной работы на объектах критической информационной инфраструктуры/информационной инфраструктуры, действий при возникновении компьютерных инцидентов и иных нештатных ситуаций работников АО «Россети ЦИУС ЕЭС», а также третьих лиц, получивших доступ к информации конфиденциального характера информационной инфраструктуры АО «Россети ЦИУС ЕЭС» на основании заключенных соглашений и договоров, в том числе к объектам критической информационной инфраструктуры ПАО «Россети», в рамках реализации договоров заключенных с указанными компаниями.

ГЛОССАРИЙ

Сокращения

В настоящем документе приняты следующие сокращения:

Сокращение	Полное наименование
АО «Россети ЦИУС ЕЭС», Общество	Акционерное общество «Россети Центр инжиниринга и управления строительством Единой энергетической системы»
АВПО	Антивирусное программное обеспечение
АРМ	Автоматизированное рабочее место
АСУ	Автоматизированная система управления
BIOS, UEFI	Набор микропрограмм, реализующих интерфейс для работы с аппаратурой компьютера и подключёнными к нему устройствами
ГИС	Геоинформационная система
ДБО	Дистанционное банковское обслуживание
ИА	Исполнительный аппарат
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
ИТС	Информационно-телекоммуникационная сеть
ЛВС	Локальная вычислительная сеть
МФУ	Многофункциональное устройство
ОРД	Организационно-распорядительный документ
ПО	Программное обеспечение
HTTPS	Протокол с поддержкой шифрования в целях повышения безопасности
SNMP Community Strings	Протокол безопасного обмена сообщениями для управления сетевыми устройствами
shared keys	Строка символов, которая используется в качестве ключа аутентификации в криптографических процессах
VPN	Виртуальная частная сеть

Термины и определения

В настоящем документе используются следующие термины и определения:

Термин	Определение
Автоматизированная система	Система, состоящая из комплекса средств автоматизации, реализующего информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование. (в соответствии с ГОСТ Р 59853-2021. Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.)
Автоматизированная система управления	Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами (в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)
Информационные ресурсы	Отдельные документы или отдельные массивы документов, документы или массивы документов в информационных системах
Информационная	Совокупность содержащейся в базах данных

система	информации и обеспечивающих ее обработку информационных технологий и технических средств (в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)
Критическая информационная инфраструктура	Совокупность имеющихся сервисов и систем, сетей, технических и программных средств, данных, автоматизированных процессов, обеспечивающих информационное обеспечение деятельности объектов ПАО «Россети» и которым присвоена одна из категорий значимости
Информационная инфраструктура	Совокупность объектов информатизации, информационных систем, сайтов, в том числе в сети «Интернет», сетей связи Общества, являющихся собственностью Общества или используемых на основании заключенных соглашений и договоров.
Кроссовое помещение	Помещение или пространство, отведенное под коммутацию (соединение) телекоммуникационного оборудования
Многофункциональное устройство (МФУ)	Устройство, сочетающее в себе функции принтера, сканера, факсимильного устройства, копировального модуля
Подразделение ИБ	Подразделение, ответственное за планирование, организацию, реализацию и контроль мероприятий по обеспечению информационной безопасности. Таким подразделением является Управление экономической и региональной безопасности Общества. Ответственные за обеспечение ИБ лица назначаются соответствующим ОРД Общества
Пользователь	Лицо, участвующее в функционировании информационной системы или использующее результаты её функционирования
Средства вычислительной техники	Совокупность программных технических элементов систем обработки данных, способных функционировать самостоятельно или в

	составе других систем
--	-----------------------

1 Общие положения

1.1. Субъектами, на которых распространяется действие настоящих Правил, являются (далее – Работники):

- работники АО «Россети ЦИУС ЕЭС»;
- физические лица, с которыми заключены срочные договоры гражданско-правового характера;
- физические лица, выполняющие действия в отношении объектов информационной инфраструктуры (серверные, кроссовые и иные помещения), в том числе с целью уборки помещений, выполнения работ по техническому обслуживанию, проведения аудита, прохождения стажировки и т.д. и их отдельными элементами Общества;
- работники юридических лиц, выполняющих работы на объектах информационной инфраструктуры или в отношении объектов информационной инфраструктуры Общества в соответствии с условиями заключенных договоров, иных законных основаниях.

1.2. Объектами защиты в контексте обеспечения безопасности информационной инфраструктуры Общества и информации конфиденциального характера являются:

- корпоративные информационные системы (включая, но не ограничиваясь, машинные носители информации, автоматизированные рабочие места, серверы, средства обработки буквенно-цифровой, графической, видео- и речевой информации, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие устойчивость финансово-хозяйственной деятельности Общества;
- автоматизированные системы управления (включая, но не ограничиваясь, автоматизированные рабочие места, промышленные серверы, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства), имеющее функции как локального, так и дистанционного управления, либо имеющее функционирующие интерфейсы сетевого взаимодействия, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие надежное снабжение потребителей электроэнергией;
- корпоративные и технологические информационно-телекоммуникационные сети (включая, но не ограничиваясь, телекоммуникационное оборудование, программное обеспечение, система управления, линии связи), формирующие единое информационное пространство и цифровую среду взаимодействия;
- цифровые устройства и периферийное оборудование (включая, но не ограничиваясь, принтеры, сканеры, IP-телефоны, цифровые камеры, смартфоны);
- сети электросвязи, используемые для организации взаимодействия объектов и передачи информации, места выхода в сеть Интернет;
- архитектура и конфигурация информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (в том числе входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, персональные данные, иная информация конфиденциального характера, в том числе представляющая коммерческую ценность в силу неизвестности третьим лицам).

1.3. Работники обязаны неукоснительно соблюдать требования настоящих Правил при работе с информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями, включая их элементы (автоматизированные рабочие места, серверы, коммутационное, сетевое и иное оборудование), а также при работе с

информацией конфиденциального характера.

1.4. Общество предпринимает разумно достаточные средства и методы технической защиты объектов информационной инфраструктуры и обрабатываемой информацией конфиденциального характера, а также другие, не противоречащие законодательству Российской Федерации, меры.

1.5. С целью повышения уровня внимания Работников к вопросам обеспечения безопасности информации, в местах для информирования (информационных стендах, досках) на территории Общества (включая электросетевые объекты) должна быть размещена памятка работнику критической информационной инфраструктуры (приложение 1 к настоящим Правилам).

1.6. В случае организации посещения электросетевых объектов, административных и иных объектов Общества физическими лицами в ходе экскурсий, проверок, иных случаях, не предусматривающих заключение договоров или соглашений, должностные лица Общества, ответственные за организацию (сопровождение) такого рода посещений, должны информировать посетителей о действии настоящих Правил на территории Общества.

2 Правила работы с информацией конфиденциального характера

2.1. Информация, обрабатываемая в Обществе, делится на:

- информацию конфиденциального характера;
- иную (в том числе общедоступную) информацию.

2.2. Перечень информации конфиденциального характера определяется в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» и утверждается соответствующими ОРД Общества.

2.3. Информация, обрабатываемая на объектах информационной инфраструктуры Общества, относится к охраняемой компьютерной информации.

2.4. Информация в Обществе обрабатывается в электронном виде и на бумажных носителях.

2.5. Порядок обработки информации конфиденциального характера в Обществе определяется приказами АО «Россети ЦИУС ЕЭС» от 15.05.2012 № 76 «Об утверждении Положения о временном порядке организации работы по обеспечению защиты информации, составляющей коммерческую тайну АО «Россети ЦИУС ЕЭС», от 03.04.2015 № 44 «Об организации работ по защите информации, составляющей служебную тайну АО «Россети ЦИУС ЕЭС» и приказом АО «Россети ЦИУС ЕЭС» от 07.11.2019 № 291 «Об утверждении Положения о защите персональных данных в АО «Россети ЦИУС ЕЭС».

3 Правила безопасной работы на объектах критической информационной инфраструктуры/информационной инфраструктуры

3.1. Работникам запрещено:

3.1.1. Разглашать информацию ограниченного доступа, включая обрабатываемую на объектах КИИ, в том числе:

- осуществлять фото- и видеосъемку экранов АРМ, офисных помещений, мест расположения средств вычислительной техники в случае, если данные действия не являются необходимыми для выполнения трудовых функций, закрепленных в должностной инструкции Работника, или не предусмотрены договором между Обществом и Работником, организационно-распорядительными документами Общества;
- осуществлять скрытую аудио- и видеозапись совещаний и переговоров;
- выбрасывать информацию ограниченного доступа в печатном виде в мусорные корзины (бумажные носители должны уничтожаться с применением устройств по измельчению бумаги («шредер»)¹;
- выполнять печать и сканирование документов с информацией ограниченного доступа на общедоступных МФУ (расположенных в коридорах, залах, рекреациях, иных местах и помещениях, в которые возможен неконтролируемый доступ посторонних лиц);
- обсуждать сведения, относящиеся к информации ограниченного доступа, в присутствии третьих лиц или в местах, где такая информация может быть услышана третьими лицами;
- оставлять бумажные или электронные носители с информацией ограниченного доступа в переговорных комнатах и других общедоступных местах, включая общедоступные МФУ.

3.1.2. Использовать недоверенные устройства и ПО на АРМ, в том числе:

- осуществлять попытки самостоятельного внесения изменений в настройки операционных систем и параметров безопасности средств защиты информации, установленных на АРМ;
- использовать незарегистрированные (в том числе – личные) USB-накопители на значимых объектах КИИ;
- устанавливать не предусмотренное для выполнения рабочих обязанностей ПО (игры, медиаплееры и т.п.);
- использовать сторонние Wi-Fi сети для подключения корпоративных устройств (в том числе создавать собственные Wi-Fi и иные беспроводные сети);
- использовать некорпоративные почтовые сервисы;
- использовать личную периферийную технику (клавиатуры, мыши, принтеры, сканеры, МФУ).

3.1.3. Получать несанкционированный доступ к информационным системам и ресурсам Общества, в том числе:

¹ подпункт подлежит исполнению при обеспечении устройствами по измельчению бумаги («шредер»)

- использовать чужие учетные данные для доступа к информационным системам Общества;

- использовать уязвимости и незадокументированные возможности ПО;
- отправлять электронные письма в личных (не связанных с производственной деятельностью) целях.

3.2. Работник обязан незамедлительно сообщать в подразделение ИБ по электронной почте infosec@cius-ees.ru или телефону 7 (495) 710-60-60 (доб. 36-66) информацию о следующих фактах:

- выявлении подозрительной активности на АРМ;
- выявлении вирусной активности;
- утрате носителей служебной информации и мобильных АРМ (ноутбук, планшет, смартфон);
- раскрытии парольной информации;
- утрате или компрометации носителей сертификатов ключа проверки электронной подписи (ключевых носителей);
- обнаружении неопознанных ключевых носителей, носителей информации;
- обнаружении неопределенных технических средств (устройств) несанкционированное подключенных к АРМ, ЛВС;
- обнаружении уязвимостей в любых элементах АРМ, серверов, ЛВС, ИС и АСУ;
- обнаружении ошибок в настройке и работе ИС и АСУ, сетей связи, приводящих к доступу в области, не предусмотренной изначальной заявкой на доступ;
- обнаружении в открытом доступе в любом виде учетных данных (паролей и имен пользователей);
- обнаружении несанкционированного доступа других лиц к информации или АРМ;
- попытках получения парольной информации третьими лицами;
- прекращении работоспособности средств защиты информации.

3.3. Все оборудование, имеющее интерфейсы сетевого взаимодействия, должно быть закреплено за работниками Общества.

4 Правила работы с учетными записями

4.1. В Обществе используются 3 типа учетных записей:

- «пользователь»;
- «администратор»;
- «сервисная».

4.2. По умолчанию всем Работникам предоставляется корпоративная учетная запись типа «Пользователь», позволяющая получить доступ только к АРМ, а также доступ к системе электронного документооборота.

4.3. Доступ к информационным системам, системы планирования и ведения финансово-хозяйственной деятельности (SAP, 1C), иным ресурсам, необходимым для выполнения производственных задач осуществляется в соответствии с приказом АО «Россети ЦИУС ЕЭС» от 02.04.2021 № 125 «Об утверждении Положения по организации доступа и развитию информационных систем АО «Россети ЦИУС ЕЭС».

4.4. Доступ к автоматизированным системам управления, иным технологическим системам осуществляется в соответствии с порядком, предусмотренным эксплуатационной, проектной документацией на данные системы.

4.5. Доступ к АРМ, корпоративному персонифицированному ящику электронной почты, сетевым папкам и сети Интернет для лиц, не являющихся работниками Общества, предоставляется по заявке руководителя структурного подразделения Общества (куратора соглашения, договора) с заполненным обязательством (приложение 2 к настоящим Правилам) на имя Заместителя Генерального директора по общим вопросам после согласования заявки с подразделением ИБ.

4.6. Создание учетной записи типа «Администратор» и «Сервисная», повышение уровня доступа существующей учетной записи осуществляется по согласованию с подразделением ИБ.

4.7. Все учетные записи должны быть персонифицированы, за исключением случаев, когда необходимость работы под обезличенной учетной записью обусловлена техническими требованиями информационной системы, автоматизированной системы управления или оборудования информационно-телекоммуникационной сети.

4.8. Учетные записи, неиспользовавшиеся в течение 4 месяцев, должны быть автоматически заблокированы.

4.9. В случае прекращения трудовых отношений с Работником, учетные записи, принадлежащие Работнику, должны быть заблокированы.

4.10. Разблокирование учетных записей, сброс пароля на действующих учетных записях, предоставление доступа к учетной записи уволенного работника, иные действия с учетными записями осуществляются по согласованию с подразделением ИБ.

4.11. В случае применения механизмов двухфакторной аутентификации с использованием связанного с учетной записью телефонного номера, номер, используемый для получения второго фактора, должен принадлежать Работнику или быть закрепленным за Работником (в случае

использования корпоративных телефонных номеров Общества).

4.12. В случае необходимости использования одной (персонифицированной) учетной записи несколькими работниками Общества, подразделением – владельцем информационной системы должен быть разработан и утвержден ОРД перечень лиц, допущенных к работе в информационной системе (автоматизированной системе управления, оборудовании ИТС) под указанной учетной записью и назначен ответственный за периодическую смену пароля.

4.13. Требования к имени учетной записи:

- имя учетной записи должно быть уникальным в пределах используемой информационной системы или ПАК;
- следует избегать применения специальных символов и цифр в учетной записи, за исключением «-» и «_»;
- все учетные записи типа «администратор» должны содержать приставки «adm-» и «adm_» и иметь формат Ф_ИО или Ф-ИО администратора;
- имя учетной записи должно соответствовать стандартам и рекомендациям, установленным для информационной системы или ПАК, в которых она используется;
- имя учетной записи должно применяться для быстрой идентификации учетной записи и ее владельца;
- имя учетной записи не должно содержать информацию ограниченного доступа.

5 Правила работы с паролями

5.1. Требования к сложности (стойкости) пароля:

- строчные латинские буквы: abcd...xyz;
- прописные латинские буквы: ABCD...XYZ;
- цифры: 123...90;
- специальные символы: !%()+ и т.д.

5.2. Пароли не должны основываться на типовых шаблонах и идущих подряд на клавиатуре или в алфавите символов (qwerty, 1234567, abcdefgh и т.д.), а также не должны основываться на каком-либо одном слове, выданном идентификаторе, информации, основанной на данных о пользователе (имени, фамилии, дате рождения, паспортных данных, номерах страховок, автомобильном или телефонном номере и т.п.), названии компании, кличке животных и т.п., в том числе набранные в другой раскладке клавиатуры.

5.3. Требования к длине пароля:

— для Работников с правами «пользователя» длина пароля должна составлять не менее 15 символов;

— для Работников с правами «администратора» (локального/доменного) длина пароля должна составлять не менее 20 символов;

— для сервисных учетных записей длина пароля должна составлять не менее 20 символов;

— для разделяемых ключей шифрования (shared keys) длина пароля должна составлять не менее 32 символов (256 бит).

5.4. Периодичность обязательной смены пароля:

— пользовательских учетных записей – каждые 90 дней;

— административных учетных записей – каждые 60 дней;

— сервисных учетных записей – не реже двух раз в год;

— shared keys SNMP Community Strings (пароли, используемые в протоколах SNMP) – не реже одного раза в год.

5.5. Пароли не должны храниться и передаваться в незашифрованном виде по публичным сетям (локальная вычислительная сеть, интернет, электронная почта).

5.6. В ходе работы не должны использоваться пароли по умолчанию. Должны быть назначены пароли, отличные от установленных производителем.

5.7. При компрометации пароля, владелец учетной записи должен незамедлительно сообщить об этом ответственному работнику подразделения ИБ и сменить все пароли.

5.8. При использовании паролей запрещено:

- хранить и записывать пароли на бумаге, и том числе на предметах, а также в местах, доступных третьим лицам;
- хранить и записывать пароли в электронном виде без использования криптографической защиты;
- передавать и сообщать третьим лицам личный пароль (за исключением случаев хранения руководителями или ответственными работниками подразделений паролей в соответствии с обязанностями, указанными в положении о подразделении и (или) должностных инструкциях);
- регистрировать третьих лиц под своим паролем;
- передавать парольные фразы пользователям при помощи почтовых сообщений либо иным открытым способом через Интернет без использования парольной или криптографической защиты;
- вводить свой пароль в случае, если он может быть просмотрен случайно или намеренно третьим лицами;
- использовать одни и те же пароли для разных информационных систем (автоматизированных систем управления, оборудования информационно-телекоммуникационной сети);
- создавать учетные записи, профили на сторонних интернет-сервисах и информационных системах (включая общедоступные сервисы электронной почты) с использованием пароля от корпоративного АРМ.
- использовать функцию «Запомнить пароль» в программном обеспечении.

5.9. В случае отсутствия технической возможности использования паролей, соответствующих требованиям настоящего раздела, требования к паролям устанавливаются на этапе проектирования или разработке эксплуатационной документации на ИС, АСУ, ИТС.

6 Правила работы на АРМ

6.1. Работники должны обладать необходимыми навыками работы с используемым аппаратным и программным обеспечением.

6.2. Для выполнения производственных задач Работнику предоставляется корпоративное АРМ, включающее в себя средства вычислительной техники (персональный компьютер), виртуальные ресурсы вычислительной сети, периферийное, мобильное и иное оборудование, предусмотренное должностными обязанностями Работника и соответствующими ОРД Общества.

6.3. В случае необходимости организации АРМ для лиц, не являющихся работниками Общества, АРМ создается по обращению руководителя структурного подразделения Общества, куратора соглашения, договора после согласования с подразделением ИБ.

6.4. К ИТС Общества запрещено подключать личные средства вычислительной техники (персональный компьютер, ноутбук, смартфон, планшет, модем, роутер, точку доступа, IP видеокамеру, цифровую приставку для ТВ и т.д.) в том числе с целью зарядки, передачи файлов и т.д.

6.5. Доступ Работника к АРМ осуществляется:

- с применением персональной доменной учетной записи;
- с применением локальной персонифицированной или общей учетной записи;
- с применением средств защищенного удаленного доступа.

6.6. Использование локальных учетных записей допускается:

- в случаях, предусмотренных эксплуатационной или проектной документацией на эксплуатируемую систему;
- в случаях проведения работ по техническому обслуживанию АРМ (для работников технической поддержки);
- в отдельных случаях, после получения согласования со стороны подразделения ИБ.

6.7. Удаленное подключение к АРМ допускается:

- в случаях, предусмотренных эксплуатационной или проектной документацией на эксплуатируемую систему;
- в случаях введения ОРД Общества удаленного режима работы, за исключением подключения к АРМ, входящих в состав автоматизированных систем управления, иных технологических систем;
- в отдельных случаях, после получения согласования со стороны подразделения ИБ.

6.8. Все АРМ (включая мобильные и виртуальные) должны быть оснащены средствами антивирусной защиты.

Периодичность осуществления обязательной антивирусной проверки АРМ – не реже 1 раза в неделю.

Работники Общества обязаны осуществлять подготовку АРМ к проведению проверки автоматическими средствами АВПО в соответствии с установленным порядком (приложение 3 к настоящим Правилам).

6.9. Доступ к настройкам BIOS АРМ, настройкам МФУ, сетевого и коммутационного оборудования должен быть заблокирован.

6.10. При организации защищенного удаленного доступа к АРМ или информационным

системам с использованием механизмов двухфакторной аутентификации посредством отправки SMS-кодов не допускается использование телефонных номеров, принадлежащих третьим лицам, в том числе родственникам или знакомым работника, коллегам.

6.11. Организация удаленного подключения подрядных организаций к корпоративным АРМ осуществляется по согласованию с подразделением ИБ.

6.12. По окончании сеанса работы на АРМ или при необходимости оставления рабочего места Работник должен заблокировать экран средств вычислительной техники (блокирование экрана на персональном компьютере осуществляется нажатием сочетания клавиш Win + L или нажатием сочетания клавиш Ctrl + Alt + Del и выбором опции «Блокировать компьютер»).

6.13. При работе на АРМ запрещено:

- эксплуатировать средства вычислительной техники при отключенных или неустановленных средствах антивирусной защиты и встроенных в операционную систему средствах обеспечения безопасности (MS Windows Defender);
- оставлять рабочее место без блокирования экрана средств вычислительной техники;
- использовать АРМ в нерабочее время не по прямому назначению;
- осуществлять работу на АРМ, не удовлетворяющих требованиям информационной безопасности;
- допускать к работе на своем АРМ третьих лиц, за исключением работников службы технической поддержки и работников подразделения ИБ;
- срывать пломбы или печати, вскрывать корпус персонального компьютера, осуществлять самостоятельную сборку и разборку средств вычислительной техники;
- использовать уязвимости и недокументированные возможности установленного ПО;
- вносить изменения в аппаратную и программную конфигурацию АРМ;
- хранить личную, не имеющую отношения к выполнению должностных обязанностей, информацию на АРМ и сетевых ресурсах;
- производить загрузку АРМ с внешних и сетевых носителей;
- получать доступ к BIOS или UEFI персонального компьютера;
- использовать АРМ с локальными учетными записями;
- препятствовать работе средств защиты информации или обходить их;
- самостоятельно подключать к АРМ периферийные и внешние устройства, в том числе:
 - принтеры, сканеры и многофункциональные устройства;
 - модемы и адаптеры связи;
 - мобильные телефоны, планшеты и другие подобные устройства;
 - личные носители информации;
 - устройства двойного назначения – скрывающие встроенный функционал;
- использовать АРМ с одновременным подключением к ЛВС и другим сетям;
- оставлять средства вычислительной техники (ноутбук, смартфон, планшет) в

общедоступных местах без присмотра;

- осуществлять подключение (проводное или беспроводное) к АРМ личных мобильных устройств (смартфон, планшет, модем или другие внешние устройства), в том числе с целью зарядки;
- производить самостоятельное удаление/установку программного обеспечения на АРМ.

6.14. При увольнении Работника информация на жестком диске персонального компьютера Работника и сетевых ресурсах подлежит передаче непосредственному руководителю Работника, после чего персональный компьютер и другие средства вычислительной техники, полученные работником, должны быть сданы в структурное подразделение, осуществляющее выдачу средств вычислительной техники.

6.15. При приемке АРМ уволенного Работника должна быть выполнена процедура удаления информации и установлена новая копия операционной системы и прикладного ПО.

6.16. При передаче средств вычислительной техники в ремонт, в иных случаях передачи средств вычислительной техники третьим лицам (включая списание и утилизацию) жесткие диски должны быть демонтированы.

6.17. Передача средств вычислительной техники с жесткими дисками, передача жестких дисков в ремонт осуществляется после согласования с подразделением ИБ.

6.18. При списании, утилизации жестких дисков, иных носителей информации должна быть выполнена процедура удаления информации без возможности её восстановления.

6.19. Физический доступ в помещения с АРМ, серверные, кроссовые помещения, а также помещения с размещенными в них элементами информационной инфраструктуры должен обеспечиваться с использованием средств контроля и управления доступом или иными способами контроля, позволяющими исключить несанкционированным доступ в помещение посторонних лиц.

6.20. Доступ в помещения с АРМ, серверные и кроссовые помещения, иные помещения с размещенными элементами информационной инфраструктуры представителям подрядных организаций, контрагентов и иным лицам, не являющимся работниками АО «Россети ЦИУС ЕЭС» (в том числе с целью уборки помещений, выполнения работ по техническому обслуживанию, проведения аудита, прохождения стажировки и т.д.), предоставляется по согласованию с подразделением ИБ.

6.21. Доступ в помещения с АРМ, серверами, коммутационным оборудованием осуществляющими обработку информации технологического характера (в том числе информации о значимых объектах критической информационной инфраструктуры/информационной инфраструктуры) третьим лицам предоставляется только при непосредственном сопровождении работника, назначенного ответственным за ИБ.

7 Правила работы с информационными системами

7.1. При работе с информационными системами (автоматизированными системами управления, оборудовании информационно-телекоммуникационной сети) запрещено:

- использовать уязвимости и недокументированные возможности программного и аппаратного обеспечения;
- использовать (в любых целях) ошибки системы;
- осуществлять деструктивные воздействия на программное обеспечение и данные в информационных системах (автоматизированных системах управления);
- несанкционированно изменять или уничтожать данные в информационных системах или на внешних (отчуждаемых) носителях;
- несанкционированно устанавливать на автоматизированные рабочие места любые дополнительные программные и аппаратные компоненты и устройства;
- осуществлять доступ под чужими учетными данными;
- выполнять резервное копирование информации на личные носители, облачные сервисы, внешние сервисы электронной почты;
- публиковать в открытом доступе информацию об архитектуре и конфигурации корпоративных и технологических информационно-телекоммуникационных сетей, сетей электросвязи, используемых для организации взаимодействия объектов и передачи информации, в том числе для выхода в сеть «Интернет».

7.2. При работе с технологическими системами (в том числе автоматизированными системами управления) Работник должен уделять особое внимание безопасности информации.

7.3. Порядок работы с технологическими системами указывается в эксплуатационной или проектной документации на данные системы.

8 Правила работы в ЛВС

8.1. Работнику для выполнения служебных обязанностей предоставляется доступ в ЛВС со стационарного АРМ.

8.2. Удаленный доступ к внутрикорпоративным web-сервисам и информационным системам, в том числе с использованием сторонних средств вычислительной техники, должен осуществляться через «единое окно» по защищенному каналу связи с применением средств терминального доступа или VPN шлюза по протоколу HTTPS с применением двухфакторной аутентификации, в том числе с применением персональных сертификатов, выдаваемых удостоверяющим центром Общества.

8.3. К средствам вычислительной техники (персональный компьютер, ноутбук, планшет), с которых осуществляется удаленный доступ к информационным системам, в том числе к корпоративным АРМ, применяются все требования настоящих Правил.

8.4. В случае осуществления удаленного или локального доступа к ЛВС Общества с АРМ организаций, выполняющих работы/оказывающих услуги в интересах Общества, доступ предоставляется только при условии наличия с указанной организацией соглашения об охране и передаче информации и соглашения/условий договора о соблюдении требований настоящих Правил работниками указанной организации, а также при наличии в указанном соглашении/договоре ответственности за нарушение требований настоящих Правил. При этом АРМ указанной организации должны удовлетворять требованиям и мерам защиты информации, принятым в Обществе.

8.5. При работе в ЛВС без предварительного согласования с подразделением ИБ не допускается:

- устанавливать удаленный доступ к АРМ и ЛВС, подключать любые устройства к ЛВС;
- осуществлять доступ к ЛВС с личных устройств;
- осуществлять сетевой доступ к другим АРМ;
- подключать средства вычислительной техники, имеющие встроенные и внешние устройства беспроводной связи к ЛВС;
- подключать АРМ к беспроводным сетям.

8.6. При работе в ЛВС запрещено:

- подключать к ЛВС средства вычислительной техники с отключенными или неустановленными средствами защиты, а также с настройками, неудовлетворяющими требованиям информационной безопасности;
- проводить сканирование и анализ ЛВС и сетевых узлов;
- осуществлять перехват трафика в ЛВС;
- осуществлять атаки на АРМ, ЛВС, серверы, коммутационное и иное оборудование, включая информационные системы и автоматизированные системы управления;
- использовать уязвимости протоколов и конфигураций сетевого оборудования в ЛВС;
- организовывать точки входа и шлюзы для внешних сетей;

- создавать точки беспроводного доступа на территории Общества.

9 Правила работы в сети Интернет

9.1. Доступ к ресурсам сети Интернет предоставляется Работникам для выполнения ими трудовых функций.

9.2. Подразделение ИБ постоянно поддерживает в актуальном состоянии список запрещенных Интернет-ресурсов и блокирует доступ к ним на различных уровнях.

9.3. При работе в сети Интернет запрещено:

- обходить механизмы фильтрации запрещенных Интернет-ресурсов с помощью специализированных сервисов (анонимайзеры, прокси-серверы, VPN-серверы и сервисы, TOR-браузер и расширения с аналогичными функциями для иных браузеров);
- организовывать туннелирование внешних сетей;
- переходить по баннерам и рекламным объявлениям;
- переходить по подозрительным ссылкам;
- распространять информацию, запрещенную законодательством Российской Федерации, включая, но не ограничиваясь, материалы террористического, экстремистского, расистского, сексуального, религиозного, дискриминационного, развлекательного и другого характера, информацию о наркотических средствах, психотропных веществах и их прекурсорах, а также информацию, оскорбляющую честь, достоинство и деловую репутацию юридических и физических лиц;
- игнорировать системные сообщения АРМ и предупреждения об ошибках;
- несанкционированно размещать от имени Общества любую информацию, в том числе публиковать информацию в социальных сетях, Интернет-мессенджерах, форумах;
- использовать внешние адреса электронной почты для ведения служебной переписки;
- публиковать в сети Интернет корпоративные адреса электронной почты и телефонов работников Общества;
- приобретать, хранить и распространять информацию, запрещенную законодательством Российской Федерации, или способную причинить вред имиджу Общества или нанести материальный ущерб Обществу;
- предпринимать самостоятельные действия по устранению неполадок при подключении к сети Интернет при их возникновении;
- осуществлять работу в сети Интернет с использованием учетных записей с административными правами доступа;
- использовать ресурсы²:

² для получения исключительного доступа в случае производственной необходимости, необходимо сформировать в службу технической поддержки заявку на получение доступа с обоснованием необходимости использования данных сервисов и согласовать эту заявку с подразделением ИБ

- игрового и развлекательного характера;
 - непристойного содержания
 - социальных сетей;
 - пиринговых сетей;
 - почтовых сервисов;
 - файлообменных сервисов и облачных хранилищ, за исключением файлообменных сервисов Общества (<https://exfile.rosseti.ru/> и <https://data.fsk-ees.ru/>);
 - форумов и конференций (в части публикации сообщений);
 - сервисов коммуникаций (Telegram, WhatsApp, Instagram, Skype (за исключением корпоративной версии) и иных сервисов), за исключением случаев, когда использование такого сервиса необходимо в рамках исполнения должностных обязанностей в соответствии с положением о структурном подразделении и(или) должностной инструкцией;
 - сервисов видеотелефонной связи (Zoom, Google Meet, TrueConf и др.) за исключением использования корпоративных версий указанного программного обеспечения в рамках исполнения должностных обязанностей;
 - не связанные с исполнением трудовых функций Работников;
 - нарушающие требования действующего законодательства Российской Федерации;
 - удаленных АРМ, находящихся за пределами ЛВС, способами, выходящими за рамки утвержденных проектных решений, в том числе с использованием программ удаленного доступа (rAdmin, TeamViewer и др.);
 - снижать установленный уровень защиты информации;
 - сохранять и запускать файлы, полученные из сети Интернет, за исключением случаев, когда использование таких файлов необходимо в рамках исполнения должностных обязанностей в соответствии с положением о структурном подразделении и(или) должностной инструкцией.
- 9.4. Не допускается организация подключения к сети Интернет на АРМ и серверах технологического сегмента.

10 Правила работы с электронной почтой

10.1. Доступ к корпоративной электронной почте предоставляется Работникам только в целях исполнения трудовых функций.

10.2. Вся служебная переписка должна осуществляться только с использованием персонального адреса корпоративной электронной почты.

10.3. Работник должен проверять вложения в сообщениях электронной почты на наличие исполняемых файлов, при их наличии – не запускать исполняемый файл и сообщить о получении такого письма в подразделение ИБ. Рекомендуется открывать только вложения, имеющие следующий формат: документы (Word, Excel, PDF, txt и т.д.), изображения (JPG, PNG и т.д.).

10.4. Рекомендуется подтверждать отправку отправителем писем.

10.5. При работе с электронной почтой запрещено:

- осуществлять массовую и адресную рассылку информации, не связанной со служебной необходимостью (спам);
- направлять информацию конфиденциального характера без применения средств криптографической защиты информации по открытым (незащищенным) каналам передачи данных, в том числе через сети общего пользования и сеть Интернет;
- использовать любые другие сервисы электронной почты кроме корпоративных, если иное не предусмотрено исполнением должностных обязанностей;
- снижать установленный уровень защиты информации сообщений;
- открывать письма, поступившие от неизвестных адресатов с неизвестными вложениями;
- переходить по внешним ссылкам, указанным в электронных письмах, в случае если получение такого письма не связано с выполнением должностных обязанностей;
- осуществлять рассылку сообщений, не имеющих отношения к выполнению должностных обязанностей.
- регистрировать учетные записи, профили на сторонних Интернет-ресурсах (включая социальные сети) с указанием корпоративного адреса электронной почты, за исключением случаев, связанных с выполнением должностных обязанностей.

10.6. При получении массовой рассылки от подразделения ИБ Работники обязаны усилить бдительность к информации, получаемой по электронной почте.

10.7. При получении подозрительного письма Работник должен:

- при получении письма сомнительного содержания и/или от неизвестного пользователя с вложением не открывать его, в случае открытия – не открывать вложения, не переходить по указанным в письме ссылкам;
- при случайном открытии письма и подозрительном поведении АРМ, незамедлительно отключить АРМ от питания;
- сообщить в подразделение ИБ о факте получения и открытия вложения подозрительного письма.

11 Правила работы с носителями информации

11.1. Использование внешних носителей информации «по умолчанию» в исполнительном аппарате Общества допускается на АРМ пользователей, определенных соответствующим ОРД Общества.

11.2. В случае необходимости использования внешнего носителя, принадлежащего физическому лицу, не являющемуся работником Общества, для записи (копирования) информации на АРМ или с АРМ, руководитель структурного подразделения, с которым взаимодействует такой субъект, должен предварительно направить обращение в подразделение ИБ Общества.

В обращении указываются:

- обоснование необходимости использования внешнего носителя;
- информация, позволяющая идентифицировать подключаемый носитель (ID-устройства, производитель);
- имена АРМ, на которых будет использоваться устройство.

11.3. Работники подразделения ИБ могут блокировать порты подключения внешних носителей информации в случаях нарушения Работником требований при работе с носителями информации, при угрозе распространения вредоносного программного обеспечения, иных случаях, связанных с рисками нарушения конфиденциальности, целостности и доступности информации.

11.4. В случае использования внешнего носителя для передачи информации конфиденциального характера, такой носитель должен быть промаркирован, а вся информация на носителе должна быть зашифрована. При шифровании должны использоваться криптоалгоритмы, разрешенные к применению на территории Российской Федерации.

11.5. Учет и маркировка носителей, содержащих информацию конфиденциального характера (в том числе персональные данные), осуществляется уполномоченным работником подразделения ИБ.

11.6. По достижению целей обработки информации (в том числе – конфиденциальной) на носителе, вся информация на носителе должна быть уничтожена без возможности её восстановления.

11.7. Подключение внешних носителей информации к АСУ, АРМ и серверам (в том числе коммутационному оборудованию) технологического сегмента допускается только для работников, осуществляющих эксплуатационную и техническую поддержку указанного оборудования. Используемый носитель информации должен быть промаркирован и подлежать учету.

11.8. В случае необходимости подключения внешнего носителя информации к АРМ или серверам, размещенным в технологическом сегменте и не оснащенных средствами антивирусной защиты, необходимо предварительно выполнить проверку носителя на отдельном (изолированном от технологического сегмента и сети Интернет) АРМ, с установленным АВПО с актуальными антивирусными базами.

11.9. При работе с носителями информации запрещено:

- несанкционированно подключать и использовать внешние носители информации как к АРМ и серверам, так и к другому оборудованию;
- подключать личные носители информации к АРМ;
- использовать корпоративные носители информации Общества в личных целях, в том числе для удаленной работы на личных персональных компьютерах.

12 Правила работы с носителями ключевой информации

12.1. В Обществе применяются следующие виды ключевой информации:

- усиленная квалифицированная электронная подпись;
- неквалифицированная электронная подпись.

12.2. Усиленная квалифицированная электронная подпись используется для:

- организации юридически значимого электронного документооборота;
- акцепта заявок на платеж в информационных системах Общества (АСУ Казначейство);
- дистанционного банковского обслуживания;
- организации подключения к ГИС;
- организации подключения к государственным порталам услуг;
- в иных случаях, предусмотренных законодательством Российской Федерации и ОРД Общества.

12.3. Неквалифицированная электронная подпись используется для:

- шифрования информации, в том числе сообщений электронной почты;
- организации доступа к информационным системам Общества;
- организации защищенного удаленного доступа;
- иных случаях, предусмотренных ОРД Общества.

12.4. Выпуск сертификатов ключа проверки электронной подписи осуществляется в порядке, предусмотренном соответствующим ОРД Общества.

12.5. При работе с носителями сертификата ключа проверки электронной подписи (токенами) не допускается:

- извлечение закрытого ключа из контейнера;
- передача носителя и(или) пароля на контейнер третьим лицам;
- использование чужих носителей сертификата ключа проверки электронной подписи;
- оставление носителя в АРМ по окончании сеанса работы с электронной подписью за исключением случаев, когда постоянное присутствие носителя обусловлено требованиями информационной системы и/или эксплуатационной документацией на информационную систему.

12.6. При прекращении трудовых отношений с Обществом Работник обязан сдать имеющиеся у него носители сертификата ключа проверки электронной подписи в подразделение ИБ, либо руководителю подразделения с уведомлением подразделения ИБ.

13 Правила работы с системами ДБО

13.1. Доступ к АРМ, на котором установлены системы ДБО, предоставляется только уполномоченным соответствующим ОРД работникам Общества.

13.2. АРМ, на котором установлены системы ДБО, должно размещаться в отдельном помещении, обеспеченном средствами контроля физического доступа в помещение.

13.3. Не допускается использование сети Интернет на АРМ с установленными системами ДБО, за исключением использования соединения банк-клиент.

13.4. Не допускается удаленное подключение к системам ДБО, в том числе к АРМ с установленными системами ДБО.

13.5. На АРМ должны быть установлены и настроены необходимые средства защиты информации в соответствии с условиями банковского обслуживания.

13.6. При увольнении указанного в п. 13.1. работника все учетные записи, принадлежащие данному работнику, должны быть заблокированы. В случае использования неперсонифицированной учетной записи в системе ДБО должна быть произведена смена паролей такой учетной записи, а также смена пароля к контейнеру сертификата электронной подписи и (или) блокирование (отзыв) сертификата электронной подписи, принадлежащий данному работнику.

13.7. Для размещения закрытых ключей электронной подписи (ЭП) должны использоваться только внешние извлекаемые носители информации.

13.8. Ключевой носитель должен храниться в недоступном для посторонних лиц месте, например, в запираемом металлическом шкафу (сейфе).

13.9. Не допускается использовать ключевой носитель для иных, кроме работы с системой ДБО, целей, в том числе для хранения файлов, электронных документов.

14 Контроль

14.1. Контроль за соблюдением настоящих Правил осуществляется подразделением ИБ.

14.2. Подразделением ИБ применяются автоматизированные и автоматические средства для контроля и предотвращения утечки информации на АРМ Работников и в ЛВС, контроля доступа к информационным системам (включая удаленный доступ), а также противодействия компьютерным атакам на информационные активы Общества.

14.3. С целью контроля и противодействия попыткам несанкционированного доступа к информации конфиденциального характера и информационным системам (в том числе автоматизированным системам управления, оборудования информационно-телекоммуникационной сети, работники подразделения ИБ могут:

- привлекать работников службы охраны в случае оказания противодействия со стороны нарушителей;
 - блокировать без предупреждения с обязательным уведомлением по электронной почте в службу технической поддержки доступ Работников к:
 - ЛВС;
 - АРМ;
 - сети Интернет;
 - ИТС;
 - информационным системам;
 - приостанавливать действие сертификата ключа проверки электронной подписи Работника;
 - требовать от Работника лично (с уведомлением руководителя Работника) или через непосредственного руководителя Работника предоставления объяснений по выявленным фактам нарушений настоящих Правил;
 - требовать от Работника прекращения работы с АРМ, в том числе через непосредственного руководителя Работника;
 - требовать от Работника предоставления носителей информации и средств вычислительной техники, вверенных ему Обществом;
 - подготавливать представление для привлечения Работника к ответственности за нарушение настоящих Правил;
 - получать доступ к информации, обрабатываемой на АРМ Работника и сетевых ресурсах, в том числе сетевых папках структурных подразделений Общества без уведомления Работника и (или) руководителя структурного подразделения – владельца сетевого ресурса;
 - осуществлять изъятие средств вычислительной техники и носителей информации, числящихся за Работником и принадлежащих Обществу.
- 14.4. В случае выявления вредоносного программного обеспечения, в том числе по результатам работы АВПО, подразделение ИБ проводит следующие мероприятия:
- для снижения угрозы распространения вредоносного программного обеспечения отключают АРМ от ЛВС;
 - производят проверку АРМ с использованием АВПО, в том числе независимо от подключения к сети Интернет;
 - проводят исследование обнаруженного вредоносного программного обеспечения, в том числе выделенного (перемещенного в карантин), путем изучения описания его негативных воздействий, найденного в сети «Интернет»;
 - получают объяснения от лиц, осуществлявших работу на АРМ, на котором было обнаружено вредоносное программное обеспечение;

- направляют уведомление заместителю Генерального директора по безопасности АО «Россети ЦИУС ЕЭС» и руководителю Управления экономической и региональной безопасности АО «Россети ЦИУС ЕЭС» для принятия решения о дальнейшем ходе разбирательства.

14.5. В целях совершенствования мер по обеспечению информационной безопасности, работники подразделения ИБ постоянно тестируют действие технических средств защиты информации, направленных на выявление угроз и блокирования несанкционированного доступа к информации конфиденциального характера.

14.6. Работники подразделения ИБ, в случае выявления действий, противоречащих законодательству Российской Федерации в области обеспечения информационной безопасности, должны фиксировать их, уведомлять правоохранительные органы, оказывать содействие правоохранительным органам, в том числе при возбуждении административных и уголовных дел по фактам выявленных правонарушений.

15 Ответственность

15.1. Работники Общества несут персональную ответственность за соблюдение настоящих Правил.

15.2. По представлению подразделения ИБ на имя Заместителя Генерального директора по безопасности АО «Россети ЦИУС ЕЭС» к Работнику могут быть применены дисциплинарные взыскания в порядке, установленном законодательством Российской Федерации.

15.3. При принятии решения о привлечении Работника к дисциплинарной ответственности должна учитываться тяжесть совершенного проступка и обстоятельства, при которых проступок был совершен.

Приложение № 2
к Договору № _____
от _____

Протокол согласования стоимости оказываемых услуг

Услуги, выполняемые ежемесячно

Наименование услуг	Стоимость в месяц без НДС (руб.)
1.Сопровождение автоматизированной системы хранения данных, в том числе:	
1.1. Обеспечение работоспособности СХД	
1.2. Поддержка Пользователей СХД	
1.3. Администрирование СХД	
НДС (в соответствии с законодательством Российской Федерации)	
Итого ежемесячная стоимость услуг, в том числе НДС, руб.	

ИТОГО: _____ (_____) рублей __ копеек в месяц, *в том числе НДС (НДС рассчитывается в соответствии с законодательством Российской Федерации).

ЗАКАЗЧИК:

ИСПОЛНИТЕЛЬ:

_____/ Кононов А.Н./
М.П.

_____/_____
М.П.

Форма Акта сдачи-приемки услуг по ежемесячному сопровождению СХД

Акт № _____ от _____
сдачи-приемки оказанных услуг по договору оказания услуг по сопровождению
автоматизированной системы хранения данных № _____ от _____ г.

Сопровождение СХД

Отчетный период: _____

Мы, _____, нижеподписавшиеся, _____, представитель _____ ИСПОЛНИТЕЛЯ
_____, действующий на основании _____, с одной
стороны и представитель ЗАКАЗЧИКА _____, действующий на основании
Доверенности №__ от __.__.20__ г. с другой стороны составили настоящий акт в том, что оказанные в
_____ (указывается отчетный месяц) услуги удовлетворяют требованиям и условиям договора.

Услуги выполняемые ежемесячно

Наименование услуг	Стоимость в месяц без НДС (руб.)
1.Сопровождение автоматизированной системы хранения данных, в том числе:	
1.1. Обеспечение работоспособности СХД	
1.2. Поддержка Пользователей СХД	
1.3. Администрирование СХД	
НДС (в соответствии с законодательством Российской Федерации)	
Итого ежемесячная стоимость услуг, в том числе НДС, руб.	

ИТОГО за отчетный период: _____ (_____)
рублей в месяц.

Стороны подтверждают, что не имеют взаимных претензий в связи с выполнением
Исполнителем своих обязательств по настоящему Договору.

Настоящий Акт составлен в 2 (двух) экземплярах, по одному для каждой из Сторон, имеющих
одинаковую юридическую силу.

От ЗАКАЗЧИКА:

От ИСПОЛНИТЕЛЯ:

_____/_____
м.п.

_____/_____
м.п.

Форму согласовали
ЗАКАЗЧИК:

ИСПОЛНИТЕЛЬ:

_____/ Кононов А.Н./
м.п.

_____/_____
м.п.

Форма справки о цепочке собственников*

(наименование организации)

№	Информация об организации						№	Информация о цепочке собственников организации (включая конечных бенефициаров)							
	ИНН	ОГРН	Наименование (краткое)	Код ОКВЭД	Ф.И.О. руководителя	Серия и номер документа, удостоверяющего личность руководителя		ИНН	ОГРН	Наименование/ Ф.И.О.	Адрес регистрации	Серия и номер документа, удостоверяющего личность (для физических лиц)	Руководитель/ участник/ акционер/ бенефициар	Размер доли (для участников/ акционеров/ бенефициаров)	Информация о подтверждающих документах (наименование, реквизиты и т.д.)***
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
							1.1.								
							1.1.1								
							1.1.2								
							1.1.3								
							1.1.3.1								
							1.1.3.2								
							...								
							1.2								
							1.2.1								
							1.2.2								
							1.2.3								

Примечания:

(подпись уполномоченного представителя)

(Ф.И.О. и должность подписавшего)

М.П.

* В отношении контрагентов, являющихся зарубежными публичными компаниями мирового уровня, а также публичных акционерных обществ, чьи акции котируются на биржах, либо с числом акционеров более 50, указываются данные о бенефициарах (в том числе конечных) и акционерах, владеющих более 5 % акций указанных обществ либо размещается прямая ссылка на общедоступный источник, посредством которого может быть установлена соответствующая информация. В отношении акционеров, владеющих пакетами акций менее 5 %, допускается указание общей информации о количестве таких акционеров.

Изменение формы справки недопустимо.

Указывается полное наименование юридического лица с расшифровкой его организационно-правовой формы.

Графы (поля) таблицы должны содержать информацию, касающуюся только этой графы (поля).

В случае если одним или несколькими участниками/учредителями/акционерами контрагента являются юридические лица, то в зависимости от организационно-правовой формы, необходимо раскрыть цепочку их участников/учредителей/акционеров с соблюдением нумерации и представить копии подтверждающих документов для всей цепочки с их указанием.

При заполнении паспортных данных указывается только серия и номер паспорта в формате XXXX XXXXXX.

** 1.1, 1.2 и т.д. - собственники участника (собственники первого уровня);

1.1.1, 1.1.2, 1.1.3 - собственники организации 1.1 (собственники организации второго уровня) и далее - по аналогичной схеме до конечного бенефициарного собственника (пример 1.1.3.1).

*** В качестве подтверждающего документа могут быть представлены, например: выписка из ЕГРЮЛ, ЕГРИП, решение (протокол) о назначении исполнительного органа, выписка из реестра акционеров (список лиц, зарегистрированных в реестре владельцев ценных бумаг) и т.п.

Форму предоставления информации согласовали:

ЗАКАЗЧИК:

ИСПОЛНИТЕЛЬ:

_____/ Кононов А.Н./

М.П.

_____/ _____/

М.П.

**Соглашение
о передаче и охране информации, составляющей коммерческую тайну**

г. Москва

Акционерное общество «Россети Центр инжиниринга и управления строительством Единой энергетической системы», именуемое в дальнейшем «**Обладатель информации**», в лице Заместителя генерального директора по общим вопросам Кононова Александра Николаевича, действующего на основании доверенности 13.02.2026 №1498/ХД, и _____, именуемое в дальнейшем «**Контрагент**», в лице _____, действующего на основании _____, с другой стороны, именуемые в дальнейшем «**Стороны**», заключили настоящее Соглашение о нижеследующем.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Соглашение - настоящее Соглашение о передаче и охране информации, составляющей коммерческую тайну, с учетом изменений и дополнений, вносимых Сторонами в соответствии с подпунктом 6.6 Соглашения. Все ссылки в тексте Соглашения на разделы и пункты понимаются как ссылки на разделы и пункты настоящего Соглашения.

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Обладатель информации, составляющей коммерческую тайну - сторона Соглашения, которая владеет информацией, составляющей коммерческую тайну на законном основании, ограничившая доступ к этой информации и установившая в отношении этой информации режим коммерческой тайны.

Контрагент - сторона Соглашения, которой Обладатель информации, составляющей коммерческую тайну, передал Информацию.

Информация, составляющая коммерческую тайну (Информация) - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Доступ к информации, составляющей коммерческую тайну - ознакомление определенных лиц с информацией, составляющей коммерческую тайну с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача информации, составляющей коммерческую тайну - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Разглашение информации, составляющей коммерческую тайну - действие или бездействие, в результате которых Информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации.

Уничтожение информации, составляющей коммерческую тайну - действия Стороны Соглашения, направленные на приведение в предусмотренном Соглашением

порядке Информации в состоянии, исключающее возможность ее использования и восстановления.

2. ПРЕДМЕТ СОГЛАШЕНИЯ

2.1. На условиях Соглашения Владелец информации передает Контрагенту Информацию, а Контрагент обязуется обеспечить защиту Информации путем исключения доступа к Информации любых третьих лиц без согласия Владельца информации и надлежащего использования Информации работниками Контрагента без нарушения режима коммерческой тайны, установленного у Контрагента и отвечающего нормам, предусмотренным Федеральным законом «О коммерческой тайне» от 29.07.2004 № 98-ФЗ. Факт передачи Информации удостоверяется подписанием Сторонами Акта приема-передачи Информации *(по форме в соответствии с Приложением 1 к настоящему Соглашению)*.

2.2. Настоящее Соглашение определяет порядок передачи Информации и условия принятия Контрагентом мер по обеспечению конфиденциальности и использованию Информации, которая будет в течение срока действия Соглашения передана Контрагенту Владелелем информации или которая иным образом станет известной Контрагенту в рамках отношений Сторон, связанных с исполнением договора № 23-7061 от _____ (далее - Основной договор).

2.3. Положения настоящего Соглашения распространяются на информацию, составляющую коммерческую тайну Владельца информации независимо от вида носителя, на котором она зафиксирована.

2.4. Информации, составляющей коммерческую тайну, присваивается гриф «Коммерческая тайна».

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. Владелец информации вправе:

3.1.1. Относить информацию к информации, составляющей коммерческую тайну, определять перечень и состав такой информации.

3.1.2. Использовать Информацию для собственных нужд в порядке, не противоречащем законодательству Российской Федерации.

3.1.3. Разрешать или запрещать доступ к Информации, определять порядок и условия доступа к Информации.

3.1.4. Без согласования с Контрагентом, но с последующим уведомлением устанавливать, изменять и отменять в письменной форме режим коммерческой тайны в соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

3.1.5. Требовать от Контрагента и его работников, получивших доступ к Информации соблюдения обязанностей по охране ее конфиденциальности.

3.1.6. Требовать от работников Контрагента, получивших доступ к Информации в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности Информации.

3.1.7. Защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами Информации, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

3.2. Контрагент вправе в соответствии с законодательством Российской Федерации самостоятельно определять способы защиты Информации, переданной ему по настоящему Соглашению. Однако при этом совместно должно быть обеспечено выполнение следующих условий:

- исключение доступа к Информации любых лиц без согласия Владельца информации;
- возможность использования Информации работниками Контрагента без нарушения режима коммерческой тайны.

3.3. Контрагент обязан:

3.3.1. Ограничивать доступ к Информации, полученной в рамках настоящего Соглашения путем установления контроля за соблюдением режима коммерческой тайны.

3.3.2. Вести учет лиц, получивших доступ к Информации.

3.3.3. Незамедлительно сообщить Обладателю информации о допущенном Контрагентом либо ставшем ему известным факте разглашения или угрозы разглашения, незаконном получении или незаконном использовании Информации третьими лицами.

3.4. Информация может быть передана только тем работникам Контрагента, доступ которых к Информации необходим в рамках отношений Сторон, указанных в подпункте 2.2, и только в той части, в которой это необходимо. Перечень указанных работников Контрагента должен быть передан Обладателю информации заблаговременно до предоставления им доступа к Информации. В этих целях Контрагент обязан:

- ознакомить под расписку (*по форме в соответствии с Приложением 2 к настоящему Соглашению*) работника, доступ которого к информации, составляющей коммерческую тайну необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, принадлежащей Обладателю информации, а также с установленным Обладателем информации режимом коммерческой тайны и с мерами ответственности за его нарушение;

- создать работнику необходимые условия для соблюдения им установленного Обладателем информации режима коммерческой тайны.

3.5. Контрагент не должен разглашать, передавать, каким-либо способом делать известной или давать свое разрешение на использование Информации любым третьим лицам без письменного согласия Обладателя информации.

В случае письменного согласия Обладателя информации на использование Информации третьим лицом, Контрагент должен обеспечить, чтобы такое лицо до получения доступа к Информации приняло на себя письменные обязательства по неразглашению Информации в объеме не меньшем, чем установлено в Соглашении. Контрагент должен заблаговременно передать Обладателю информации заверенную копию соглашения о конфиденциальности, подписанного таким третьим лицом.

Передача Информации по открытым каналам телефонной, телеграфной, факсимильной связи и сети Интернет без принятия соответствующих мер защиты, удовлетворяющих обе Стороны, **запрещена**.

3.6. Стороны заблаговременно информируют друг друга о требованиях к настоящему Соглашению, предъявляемых локальными нормативными правовыми актами Сторон к защите Информации в объеме, необходимом для выполнения Соглашения, а также об изменениях в таких локальных нормативных правовых актах.

4. ОТВЕТСТВЕННОСТЬ И РАЗРЕШЕНИЕ СПОРОВ

4.1. Контрагент в полном объеме несет ответственность за нарушение обязательств по сохранению Информации в рамках Соглашения при разглашении Информации его работниками и третьими лицами, получившими доступ к такой Информации в соответствии с разделом 3 настоящего Соглашения.

4.2. В случае неисполнения или ненадлежащего исполнения Контрагентом (включая его работников) обязательств, предусмотренных разделом 3 настоящего Соглашения, Контрагент обязан уплатить штраф в размере 10 (десяти) % от цены Основного договора, указанного в подпункте 2.2 настоящего Соглашения, за каждый случай неисполнения или ненадлежащего исполнения указанных обязательств, а также полностью возместить Обладателю информации убытки, причиненные таким нарушением обязательств в полной сумме сверх суммы штрафа.

Уплата штрафа и возмещение убытков не освобождает Стороны от выполнения ими обязательств и принятия мер, направленных на устранение нарушений.

4.3. При разглашении Информации или наличии угрозы ее разглашения Контрагент обязан незамедлительно уведомить об этом Обладателя информации.

4.4. При проведении расследования фактов разглашения Информации или

обстоятельств, свидетельствующих о нарушении Соглашения по вине Контрагента, Владелец информации вправе направлять к Контрагенту своих работников, осуществляющих деятельность в области защиты информации. В этом случае оплата расходов, связанных с командированием таких специалистов или привлечением по согласованию Сторон независимых экспертов, производится Контрагентом, допустившим утерю или разглашение Информации.

4.5. В случаях, предусмотренных законодательством Российской Федерации, Владелец информации вправе проводить проверки соблюдения Контрагентом обязательств по защите Информации.

4.6. В случае если третье лицо предъявит иск или предпримет действия на предмет раскрытия Информации, Контрагент немедленно уведомит об этом Владельца информации.

4.7. В случае реорганизации Контрагента (слияние, присоединение, разделение, выделение, преобразование) обязательства по сохранению Информации, переданной в рамках Соглашения, переходят к вновь образованному юридическому лицу или сохраняются за Контрагентом в соответствии с разделительным балансом (передаточным актом), копию которого Контрагент обязан незамедлительно предоставить Владелцу информации, в противном случае Контрагент (его правопреемник) обязуется возместить Владелцу информации понесенные им убытки в связи с разглашением Информации.

4.8. Любые споры и разногласия между Сторонами, касающиеся Соглашения, которые не могут быть урегулированы ими путем консультаций и переговоров, должны быть переданы на рассмотрение Арбитражного суда г.Москвы. К отношениям Сторон, не урегулированным Соглашением, применяется законодательство Российской Федерации.

5. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

5.1. Настоящее Соглашение вступает в силу после его подписания Сторонами и действует до полного прекращения Сторонами обязательств, связанных с исполнением договора оказания услуг по сопровождению автоматизированной системы хранения данных № _____ от _____.

5.2. Обязательства по обеспечению установленного Владелцем информации режима коммерческой тайны, предусмотренные Соглашением, сохраняют силу в течение 5 (пяти) лет после истечения срока действия Соглашения.

6. ПРОЧИЕ УСЛОВИЯ

6.1. Контроль соблюдения обязательств по Соглашению возлагается³:

у Контрагента на: _____;

у Владельца информации на: Заместителя генерального директора по общим вопросам Кононова Александра Николаевича.

6.2. Все уведомления и сообщения, адресуемые Сторонами друг другу в соответствии с Соглашением, должны быть совершены в письменной форме и направлены заказным письмом, доставлены курьером или переданы уполномоченным представителем Сторон по следующим адресам:⁴

Владелец информации – Акционерное общество «Россети Центр инжиниринга и управления строительством Единой энергетической системы» (АО «Россети ЦИУС ЕЭС»), 121353, г. Москва, Москва, ул. Беловежская, д. 4.

Контрагент – .

6.3. Владелец информации настоящим гарантирует, что он обладает всеми правами в отношении Информации, включая право раскрывать ее Контрагенту на условиях Соглашения.

6.4. Контрагент гарантирует наличие у него организационных и технических мер и возможностей по обеспечению защиты получаемой Информации.

³ Указываются Ф.И.О. и должность работников.

⁴ Указываются полные (включая почтовый индекс) адреса доставки корреспонденции.

6.5. Информация является собственностью Обладателя информации. Обладатель информации вправе потребовать от Контрагента вернуть ему всю Информацию или любую ее часть в любое время, направив Контрагенту уведомление в письменной форме. В течение 15 (пятнадцати) календарных дней после получения такого уведомления, а также незамедлительно после вынесения соответствующим органом (учредители, орган юридического лица, суд и т.д.) решения о ликвидации Контрагента, Контрагент обязан за свой счет обеспечить возврат Обладателю информации всех оригиналов носителей такой Информации. Все копии такой Информации и ее воспроизведения в любой форме, находящиеся в распоряжении Контрагента, а также в распоряжении лиц, которым Информация была передана в соответствии с Соглашением, должны быть уничтожены Контрагентом (с обязательным письменным, с приложением подтверждающих документов (копий), уведомлением о данном факте Обладателя информации) с учетом порядка, определенного в разделе 7 настоящего Соглашения.

6.6. Любые изменения и дополнения к Соглашению действительны лишь при условии, что они совершены в письменной форме и подписаны надлежащим образом уполномоченными на то представителями Сторон, за исключением случаев изменения условий настоящего Соглашения в порядке, предусмотренном подпунктом 6.11. настоящего Соглашения

6.7. Настоящее Соглашение представляет собой исчерпывающую договоренность Сторон по предмету Соглашения. С момента подписания Соглашения все предыдущие переговоры и переписка по нему теряют силу.

6.8. Ни одна из Сторон не вправе передавать третьим лицам полностью или частично свои права и обязанности по Соглашению без предварительного письменного согласия другой Стороны.

6.9. Недействительность или невозможность исполнения любого положения Соглашения не влияет на действительность или возможность исполнения других положений Соглашения и Соглашения в целом.

6.10. Настоящее Соглашение составлено и подписано в двух экземплярах на русском языке, имеющих равную юридическую силу, по одному для каждой из Сторон.

6.11. В части, не урегулированной настоящим Соглашением, Стороны руководствуются Положением о временном порядке организации работы по обеспечению защиты информации, составляющей коммерческую тайну АО «Россети ЦИУС ЕЭС» (далее - Положение), утвержденным приказом АО «Россети ЦИУС ЕЭС» от «15» мая 2012 № 76 «Об утверждении Положения о временном порядке организации работы по обеспечению защиты информации, составляющей коммерческую тайну АО «Россети ЦИУС ЕЭС». Подписанием настоящего Соглашения Стороны подтверждают ознакомление с Положением. При условии получения работником Контрагента письменного уведомления Обладателя информации о внесении изменений в Положение, изменения в условия настоящего Соглашения в указанной части являются вступившими в силу с даты получения указанного письменного уведомления.

7. ПОРЯДОК УНИЧТОЖЕНИЯ ИНФОРМАЦИИ

7.1. Уничтожение Информации производится механическим способом комиссией Сторон с участием лиц, указанных в подпункте 6.1 настоящего Соглашения, с составлением актов «об уничтожении».

7.2. Уничтожение документов, составляющих коммерческую тайну, представленных на материальных носителях в электронном виде, производится с использованием специального программного обеспечения, не позволяющего восстановить информацию комиссией Сторон с участием лиц, указанных в подпункте 6.1 настоящего Соглашения, с составлением актов «об уничтожении».

8. ПРИЛОЖЕНИЯ

Неотъемлемой частью настоящего Соглашения являются следующие приложения:

-
- Приложение 1: форма Акта приема-передачи Информации;
 - Приложение 2: форма Расписки работника Контрагента, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей.

9. РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

Обладатель информации:

АО «Россети ЦИУС ЕЭС»

ИНН 7728645409

КПП 774550001

Юридический адрес:

121353, г. Москва, вн.тер.г.

муниципальный округ Можайский, ул.

Беловежская, д. 4

Почтовый адрес: 121353, г. Москва,

вн.тер.г. муниципальный округ

Можайский, ул. Беловежская, д. 4

Тел/факс +7 (495)710-60-60

адрес электронной почты cius@fsk-ees.ru

р/с 40702810738120011798

в ПАО Сбербанк г. Москва

к/с 30101810400000000225

БИК 044525225

Контрагент:

ИНН

КПП

ОГРН

Юридический адрес:

Банковские реквизиты:

БИК

р/с

К/С

Электронная почта:

_____/ Кононов А.Н./

М.П.

_____/ _____/

М.П.

Наименование Контрагента:

Наименование Обладателя информации:
АО «Россети Центр инжиниринга и управления
строительством Единой энергетической системы»
ИНН 7728645409
121353, г. Москва, Москва, ул. Беловежская, д. 4.

ФОРМА

АКТ

приема-передачи информации

к договору № _____ от _____ г.

АО «Россети ЦИУС ЕЭС», именуемое в дальнейшем «Обладатель информации» в лице _____, действующего на основании _____, и (*наименование Контрагента*) в лице _____, действующего на основании _____, совместно именуемые «Стороны», составили настоящий акт о нижеследующем:

1. Обладателем информации передан, а Контрагентом получен на условиях Соглашения № _____ от «____» _____ 20__ г. о передаче и охране информации, составляющей коммерческую тайну, следующий перечень информации:

- 1.1. _____;
- 1.2. _____;
- 1.3. _____;

.....

2. Указанный в п. 1 настоящего Акта приема-передачи перечень информации передан (*наименование Контрагента*) в рамках отношений, связанных с исполнением договора № _____ от _____ 20__ г.

3. Настоящий акт составлен в двух идентичных экземплярах, имеющих одинаковую юридическую силу. Настоящий акт с момента подписания его сторонами становится неотъемлемой частью Соглашения № _____ от «____» _____ 20__ г.

Обладатель информации

Контрагент

М.П.

М.П.

Форму Акта приема-передачи информации согласовали

Обладатель информации

Контрагент

_____/ Кононов А.Н./
М.П.

_____/_____
М.П.

ФОРМА

РАСПИСКА

работника Контрагента, доступ которого к информации, составляющей коммерческую тайну необходим для выполнения им своих трудовых обязанностей

Я, _____
(фамилия, имя, отчество)

(должность)

Настоящим обязуюсь:

1. В период работы в (*наименование Контрагента*), на условиях Соглашения о передаче и охране информации, составляющей коммерческую тайну № _____ от «____» _____ 20__ г. (далее - Соглашение), использовать исключительно в связи с исполнением трудовых обязанностей составляющую коммерческую тайну АО «Россети ЦИУС ЕЭС» информацию согласно приведенному ниже перечню (далее - Информация), переданную (*наименование Контрагента*) в рамках отношений, связанных с исполнением договора № _____ от _____ 20__ г.

Перечень Информации:

1. _____;
2. _____;

.....

2. Не разглашать Информацию и не использовать Информацию в личных целях без письменного согласия АО «Россети ЦИУС ЕЭС».
3. Не разглашать Информацию после прекращения трудового договора с (*наименование Контрагента*) в течение пяти лет.
4. Возместить доказанные причиненные АО «Россети ЦИУС ЕЭС» в результате разглашения по моей вине Информации убытки в соответствии с законодательством Российской Федерации и условиями Соглашения.
5. Передать (*наименование Контрагента*) при прекращении (расторжении) трудового договора имеющиеся в моем пользовании материальные носители информации, содержащие Информацию.

« » _____ 20__ г.
(дата)

(подпись)

С Положением о временном порядке организации работы по обеспечению защиты информации, составляющей коммерческую тайну АО «Россети ЦИУС ЕЭС» (далее - Положение), утвержденным приказом АО «Россети ЦИУС ЕЭС» от «15» мая 2012 № 76 «Об утверждении Положения о временном порядке организации работы по обеспечению защиты информации, составляющей коммерческую тайну АО «Россети ЦИУС ЕЭС», ознакомлен(а).

« » _____ 20__ г.
(дата)

(подпись)

Форму Расписки согласовали
Обладатель информации

Контрагент

_____/ Кононов А.Н./
М.П.

_____/_____
М.П.

Приложение № 6
к Договору № _____
от _____

ФОРМА
Согласие на обработку персональных данных
от «_____» _____ 20__ г.

Настоящим _____
(указывается полное наименование победителя закупочной процедуры

(потенциального контрагента), контрагента)

Адрес регистрации: _____

Свидетельство о регистрации: _____

ИНН _____

КПП _____

ОГРН _____

в лице _____
(указываются Ф.И.О., адрес, номер основного документа, удостоверяющего личность,

сведения о дате выдачи указанного документа и выдавшем его органе)*

действующего на основании _____, дает свое согласие Акционерному обществу «Россети Центр инжиниринга и управления строительством Единой энергетической системы (АО «Россети ЦИУС ЕЭС»), зарегистрированному по адресу: 121353, г. Москва, вн. тер. г. муниципальный округ Можайский, ул. Беловежская, д. 4, и Публичному акционерному обществу «Федеральная сетевая компания - Россети» (ПАО «Россети»), зарегистрированному по адресу: 121353, г. Москва, вн. тер. г. муниципальный округ Можайский, ул. Беловежская, д. 4, в отношении следующего перечня персональных данных руководителей и собственников (участников, учредителей, акционеров), в том числе конечных бенефициаров, участника закупки (потенциального контрагента)/контрагента/третьего лица, привлеченного контрагентом к исполнению своих обязательств по договору: фамилия имя отчество, серия и номер документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе, адрес регистрации, ИНН – на совершение действий, предусмотренных п. 3 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в том числе с использованием информационных систем, а также на представление указанной информации в уполномоченные государственные органы (Минэнерго России, Росфинмониторинг России, ФНС России) и подтверждает, что получил согласие на обработку персональных данных от всех своих собственников (участников, учредителей, акционеров) и бенефициаров.***

Цель обработки персональных данных: обеспечение соблюдения требований законодательства Российской Федерации, в том числе статьи 13.3 Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции», выполнение поручений Правительства Российской Федерации от 28.12.2011 № ВП-П13-9308, протокольного решения Комиссии при Президенте Российской Федерации по вопросам стратегии развития топливно-энергетического комплекса и экологической безопасности (протокол от 10.07.2012 № А-60-26-8), а также связанных с ними иных поручений Правительства Российской Федерации и решений Комиссии при Президенте Российской Федерации по вопросам стратегии развития топливно-энергетического комплекса и экологической безопасности.

Срок, в течение которого действует настоящее согласие: со дня его подписания до момента фактического достижения цели обработки либо отзыва настоящего согласия посредством письменного обращения субъекта персональных данных с требованием о прекращении обработки его персональных данных.

(Подпись субъекта персональных данных/
уполномоченного представителя)

(Ф.И.О. и должность подписавшего*)

М.П.

* Указываются фамилия, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе; фамилия, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных).

** При заключении договоров ПАО «Россети», АО «Россети ЦИУС ЕЭС» обязаны получить согласие на обработку персональных данных участника закупки (потенциального контрагента/контрагента/третьего лица, привлеченного контрагентом к исполнению своих обязательств по договору, и их руководителей, собственников (участников, учредителей, акционеров), в том числе конечных бенефициаров (фамилия, имя, отчество; серия и номер документа, удостоверяющего личность; ИНН (участников, учредителей, акционеров, руководителей)).

*** Заполнение участником закупки (потенциальным контрагентом)/контрагентом на сайте электронной торговой площадки/на бумажном носителе согласия на обработку его данных и информации о руководителе, собственниках (участниках, учредителях, акционерах) и бенефициарах исключает ответственность ПАО «Россети», АО «Россети ЦИУС ЕЭС» перед руководителем, собственником (участником, учредителем, акционером), а также бенефициаром контрагента/третьего лица, привлеченного контрагентом к исполнению своих обязательств по договору, за предоставление АО «Россети ЦИУС ЕЭС» данных о руководителе, собственниках (участниках, учредителях, акционерах), в том числе бенефициарах и бенефициарах третьего лица, привлеченного контрагентом к исполнению своих обязательств по договору, и предполагает, что контрагент получил у руководителя, своих бенефициаров и бенефициаров третьих лиц, привлеченных контрагентом к исполнению своих обязательств по договору согласие на представление (обработку) ПАО «Россети», АО «Россети ЦИУС ЕЭС» и в уполномоченные государственные органы указанных сведений.

Форму согласовали:

ЗАКАЗЧИК:

ИСПОЛНИТЕЛЬ:

_____/ Кононов А.Н./

М.П.

_____/_____/

М.П.