

город Самара

«24» 10 2025 года

Публичное акционерное общество энергетики и электрификации «Самараэнерго» (ПАО «Самараэнерго»), именуемое в дальнейшем «Заказчик», в лице заместителя генерального директора по техническим вопросам и информационным технологиям Шумана Родиона Львовича, действующего на основании доверенности № 30 от 29.12.2024 года, с одной стороны, и Публичное акционерное общество «Ростелеком» (ПАО «Ростелеком»), именуемое в дальнейшем «Исполнитель», в лице Заместителя директора филиала - директора по работе с корпоративным и государственным сегментами Самарского филиала ПАО «Ростелеком» Толочной Анастасии Николаевны, действующего на основании доверенности № 0607/29/45/24 от 19.11.2024, с другой стороны, далее вместе именуемые «Стороны», заключили настоящий договор (далее- Договор) о нижеследующем:

### 1. Предмет Договора

1.1 Исполнитель обязуется в соответствии с условиями настоящего Договора передать Заказчику на условиях простой (неисключительной) лицензии право использования программного обеспечения системы анализа защищенности информации (далее – Лицензии) и оказать услуги по внедрению программного обеспечения системы анализа защищенности информации (далее – Услуги) в соответствии со Спецификацией (Приложение № 2 к настоящему Договору) (далее – Спецификация) и Техническим заданием (Приложение № 1 к настоящему Договору) (далее – Техническое задание), а Заказчик обязуется принять и оплатить Лицензии, Услуги в соответствии с условиями настоящего Договора.

1.2 Наименование, количество, срок, на который предоставляются Лицензии, цена за единицу и общая стоимость Договора указываются в Спецификации. Спецификация является неотъемлемой частью настоящего Договора.

1.3 Заказчик гарантирует, что приобретает Лицензии в качестве конечного пользователя. Территория использования программного обеспечения – Российская Федерация

### 2. Стоимость Договора и порядок расчетов.

2.1 Стоимость Договора составляет: 10 463 171 (Десять миллионов четыреста шестьдесят три тысячи сто семьдесят один) рубль 14 копеек, в том числе НДС в сумме 1 178 461 (Один миллион сто семьдесят восемь тысяч четыреста шестьдесят один) рубль 86 копеек, в том числе:

2.1.1 Стоимость Лицензий составляет: 3 392 400 (Три миллиона триста девяносто две тысячи четыреста) рублей 00 копеек НДС не облагается на основании пп. 26 п. 2 ст. 149 НК РФ;

2.1.2 Стоимость Услуг составляет 7 070 771 (Семь миллионов семьдесят тысяч семьсот семьдесят один) рубль 14 копеек, в том числе НДС в сумме 1 178 461 (Один миллион сто семьдесят восемь тысяч четыреста шестьдесят один) рубль 86 копеек.

2.2 Стоимость Договора включает в себя стоимость Лицензий, Услуг, расходы на уплату налогов, пошлин, сборов и другие обязательные платежи, взимаемых с Заказчика в связи с исполнением Договора, и/или другие затраты, возникающие в связи с исполнением обязательств по Договору.

2.3 Заказчик производит оплату в течение 7 (семи) рабочих дней с даты приемки Лицензий, и оказанных Услуг, на основании выставленного Исполнителем счета на оплату.



2.4 Оплата по настоящему Договору производится в рублях Российской Федерации путем безналичного перечисления Заказчиком на расчетный счет Исполнителя, указанный в настоящем Договоре.

2.5 На суммы, подлежащие оплате в соответствии с настоящим Договором, проценты по статье 317.1 ГК РФ не начисляются.

### **3. Срок и порядок передачи Лицензий и оказания Услуг.**

3.1 Срок полного и окончательного оказания услуг, включая передачу Лицензий, изготовление и предоставление Заказчику всей требуемой документации не позднее 10 декабря 2025 года.

3.2 Исполнитель осуществляет передачу Заказчику Лицензий в срок не позднее 15 календарных дней с момента заключения Договора. В целях обеспечения обязательств по настоящему Договору Исполнитель одновременно с передачей Лицензий передает Заказчику надлежащим образом оформленные документы, подтверждающие и необходимые для правомерного использования Лицензий конечным пользователем.

3.3 В целях обеспечения обязательств по настоящему Договору Исполнитель сопровождает передачу Лицензий Заказчику надлежащим образом оформленными документами, подписанными уполномоченными представителями Исполнителя: счет, счет-фактура (если применимо), детализированный акт приема-передачи или детализированный УПД в 2 (Двух) экземплярах, в которых указываются наименование, артикул/парт-номер Лицензий, количество, цена, стоимость. Документы должны быть обязательно предварительно согласованы с Заказчиком.

3.4 Заказчик подписывает предоставленные Исполнителем документы: акт приема-передачи или УПД в течение 5 (Пяти) рабочих дней с даты получения указанных документов и направляет 1 (Один) подписанный экземпляр Исполнителю или в те же сроки направляет Исполнителю письменный мотивированный отказ от подписания указанных документов.

3.5 Возврат Лицензий, не соответствующих условиям настоящего Договора и/или Спецификации, Техническому заданию осуществляется Исполнителем самостоятельно и за собственный счет.

3.6 Предоставление недостающих и/или замена несоответствующих условиям настоящего Договора Лицензий осуществляется Исполнителем в течение 3 (Трех) рабочих дней с даты подписания соответствующего мотивированного отказа, если иной срок не указан в мотивированном отказе, и оформляется соответствующими документами: актом приема-передачи или УПД, счет-фактурой (если применимо).

3.7 Исполнитель не позднее 3 (трех) рабочих дней после окончания оказания Услуг обязан предоставить Заказчику: счет, счет-фактура (если применимо), акт сдачи-приемки оказанных услуг или УПД в 2 (Двух) экземплярах. Документы должны быть обязательно предварительно согласованы с Заказчиком.

3.8 Исполнитель до подписания акта сдачи-приемки оказанных Услуг или УПД должен заблаговременно согласовать с Заказчиком и передать ему в электронном виде/на электронном носителе: текстовую часть в формате Microsoft Word, а также в 2 (двух) полных, бумажных, надлежащим образом оформленных и переплетенных экземплярах, предельно детализированную документацию, полностью соответствующую всем требованиям (Приложение 1 к Договору).

3.9 В течение 7 (Семи) рабочих дней с даты получения акта сдачи-приемки оказанных Услуг или УПД, Заказчик передает Исполнителю, подписанный акт сдачи-приемки



оказанных услуг или УПД, либо письменный мотивированный отказ от приемки Услуг. В случае отказа Заказчика от приемки Услуг, последний в срок не более чем 7 (Семи) рабочих дней составляет перечень необходимых доработок и определяет сроки их выполнения. Доработки по мотивированному отказу Заказчика производятся Исполнителем своими силами и за свой собственный счет при условии, что они не выходят за пределы условий настоящего Договора. Повторное предъявление и повторная приемка Услуг после проведения доработок осуществляются в порядке, установленном для первоначальной приемки Услуг.

3.10 Заказчик, принявший результаты Услуг без проверки, не лишается впоследствии права ссылаться на недостатки результатов Услуг, которые могли быть установлены при обычном способе ее приемки (явные недостатки).

3.11 Обязательства Исполнителя считаются исполненными с даты подписания обеими Сторонами надлежащим образом оформленных в соответствии с законодательством Российской Федерации документами: акта приема-передачи или УПД, акта сдачи-приемки оказанных Услуг или УПД.

#### **4. Требования к Лицензиям, Услугам.**

4.1 Качество Лицензий должно соответствовать требованиям нормативных правовых актов Российской Федерации, условиям Договора и Спецификации.

4.2 Лицензии на момент их передачи Заказчику по акту приема-передачи или УПД должны быть свободным от прав и притязаний третьих лиц.

4.3 Исполнитель подтверждает, что Заказчику в связи с владением, использованием, распоряжением Лицензиями не потребуется получения какой бы то ни было, не предусмотренной настоящим Договором, лицензии, права пользования патентом или иное разрешение ни от Исполнителя, ни от третьих лиц, а также то, что Заказчик не обязан к каким-либо платежам, не предусмотренным настоящим Договором, в связи с использованием в Лицензиях объектов интеллектуальной собственности Исполнителя или третьих лиц.

4.4 Исполнитель должен оказать Услуги по внедрению системы анализа защищенности информации в соответствии с требованиями Технического задания (Приложение № 1 к Договору).

4.5 Исполнитель должен разработать и передать Заказчику документацию, в соответствии с требованиями Технического задания (Приложение № 1 к Договору).

#### **5. Права и обязанности Сторон**

5.1 Исполнитель обязан:

5.1.1 В течение 10 (десяти) рабочих дней после подписания настоящего Договора, представить официальным письмом и согласовать с Заказчиком список персонала для оформления допуска на территорию объекта Заказчика, удаленного доступа.

5.1.2 Выполнять запросы физического доступа на территорию Заказчика и удаленного доступа исключительно в полном соответствии условиям Приложения № 4 и Приложения № 5 к настоящему Договору.

5.1.3 Оказать услуги в составе и по ценам, указанным в Спецификации и в соответствии с Приложением № 1 к настоящему Договору.

5.1.4 Передать Заказчику Лицензии в объеме, в сроки, в порядке и на условиях, предусмотренных в настоящем Договоре и Приложениях к нему.

5.1.5 Своевременно информировать Заказчика о возникших ситуациях, препятствующих исполнению обязательств по Договору. В случае возникновения таких ситуаций Исполнитель обязан предложить Заказчику пути их решения собственными силами и за



собственный счет, при этом сроки предоставления Лицензий, требования к качеству Лицензий и конечным результатам, которые должны быть переданы Заказчику на основании Договора, а также стоимость Договора, изменению не подлежат.

5.1.6 В случае получения от Заказчика Акта об установленном расхождении по количеству и качеству Лицензий, оказанных услугах, Исполнитель обязуется выполнить законные требования Заказчика в установленный им срок, связанные с качеством и количеством переданных Лицензий, оказанных услугах.

5.1.7 Не передавать оригиналы или копии документов, полученные от Заказчика, третьим лицам без предварительного письменного согласия Заказчика.

5.1.8 Обеспечить пожарную безопасность Услуг и нести полную ответственность за соблюдение норм пожарной безопасности при их оказании. Обеспечить соблюдение сотрудниками Исполнителя внутриобъектного и пропускного режима, установленного Заказчиком.

5.1.9 Устранять своими силами и за свой счет все выявленные недостатки (дефекты) в Услугах.

5.1.10 Доставлять своих сотрудников для места оказания Услуг и гарантийного обслуживания своими силами и за свой собственный счет.

5.1.11 Обеспечить сохранение гарантийных обязательств производителя/правообладателя на Лицензии в течение всего срока оказания и по окончании оказания Услуг.

5.1.12 Обеспечить гарантийное сопровождение результата оказанных Услуг по настоящему Договору в течение 24 (Двадцати четырех) календарных месяцев от наиболее поздней даты подписания Заказчиком Актов сдачи-приемки оказанных услуг.

5.1.13 Немедленно уведомлять Заказчика о событиях и обстоятельствах, которые могут оказать негативное влияние на ход Услуг, качество Услуг, сроки завершения Услуг или не способствовать достижению характеристик и показателей объекта, извещать Заказчика о каждом случае возникновения аварийных ситуаций на объекте при оказании Услуг.

5.1.14 В случае возникновения претензий к Заказчику со стороны третьих лиц (в том числе производителя/правообладателя), возникших по вине Исполнителя и связанных с нарушением их интеллектуальных прав на Лицензии, Исполнитель принимает все необходимые меры по урегулированию претензий, а также возможных споров. Исполнитель обязуется урегулировать требования, претензии, либо иски третьих лиц, а также полностью возместить Заказчику расходы и убытки, связанные с компенсацией требований, претензий, исков третьих лиц, связанных с нарушением их интеллектуальных и иных прав в отношении использования Лицензий.

5.2 Исполнитель вправе:

5.2.1 По вопросам, имеющим отношение к предмету настоящего Договора, запрашивать и своевременно получать от Заказчика документы, сведения и другую информацию, а также устные и письменные разъяснения и объяснения, необходимые Исполнителю для качественного выполнения своих обязательств по настоящему Договору.

5.2.2 Самостоятельно определять способы оказания Услуг.

5.2.3 Требовать своевременной оплаты на условиях и в размере, определяемых настоящим Договором;

5.2.4 Оказывать Услуги по настоящему Договору до окончания срока, установленного Договором. Исполнитель официальным письмом уведомляет Заказчика о досрочном исполнении обязательств по Договору. Досрочная приемка Лицензий и Услуг



осуществляется с согласия Заказчика. Согласие Заказчика оформляется официальным письмом.

5.3 Заказчик обязан:

5.3.1 Принять и оплатить надлежащим образом переданные Лицензии в порядке и сроки, предусмотренные условиями настоящего Договора;

5.3.2 Использовать переданные Лицензии в пределах, предусмотренных настоящим Договором и документацией (при наличии), сопровождающих передачу Лицензий;

5.3.3 Заказчик не вправе изменять, приспособливать, транслировать, применять обратный инжиниринг, перепроектировать, декомпилировать, дизассемблировать, демонтировать и иным образом пытаться обнаружить, восстановить исходный код программных продуктов Лицензий;

5.4 Заказчик обязуется не воспроизводить любую часть программного обеспечения программного обеспечения системы анализа защищенности информации, за исключением случаев, прямо предусмотренных правом пользования производителем/правообладателем.

## **6. Гарантийные обязательства.**

6.1 Исполнитель гарантирует, что обладает всеми необходимыми правами и полномочиями для исполнения обязательств по договору.

6.2 Исполнитель гарантирует, что действует в пределах прав и полномочий, предоставленных ему Правообладателем (лицом, надлежаще уполномоченным Правообладателем), и на момент предоставления Заказчику Лицензий обладает ими в необходимом объеме. Исполнитель гарантирует, что Заказчик не обязан производить какие-либо выплаты Правообладателю для целей использования Лицензий.

6.3 Исполнитель гарантирует, что возместит Заказчику все документально подтвержденные убытки, понесенные им в случае возникновения обоснованных претензий со стороны третьих лиц и связанные с нарушением их прав на интеллектуальную собственность, возникшие по вине Исполнителя.

6.4 Исполнитель гарантирует, что все исключительные права на Лицензии признаны и защищены законодательством Российской Федерации и международными соглашениями об авторских правах, положениями иных законов и международных договоров в области интеллектуальной собственности. Исполнитель гарантирует, что поставленные Лицензии не нарушают права пользования третьих лиц, в том числе интеллектуальные права, не будут нарушены.

6.5 Исполнитель гарантирует, что программное обеспечение анализа защищенности информации удовлетворяет всем техническим требованиям, приведенным в Таблице № 1 Приложения № 1 к Договору. В случае, если в процессе использования данного программного обеспечения Заказчиком выяснится, что какие-либо из перечисленных требований не выполняются данным программным обеспечением или не содержатся в функциональном составе программного обеспечения, Заказчик вправе расторгнуть Договор в одностороннем порядке и потребовать от Исполнителя возмещения стоимости Договора в сумме, указанной в п. 2.1 и убытков в полном размере, связанных с простоями Заказчика.

6.6 Если в течение гарантийного срока использования Лицензий Заказчик выявит недостатки, которые не могли быть установлены при его приёме согласно условиям настоящего Договора, Заказчик вправе по своему выбору потребовать от Исполнителя: безвозмездного устранения выявленных недостатков силами и за счёт Исполнителя; возмещения своих расходов на устранение недостатков Лицензий.



6.7 Гарантийное сопровождение предоставляется по рабочим дням в рабочее время Заказчика: с 8:00 до 17:00 местного, Самарского времени, понедельник – пятница, за исключением общегосударственных выходных и праздничных дней.

## **7. Ответственность и права Сторон.**

7.1 За неисполнение или ненадлежащее исполнение условий Договора Стороны несут ответственность, предусмотренную законодательством Российской Федерации.

7.2 В случае нарушения Заказчиком сроков оплаты Исполнитель вправе потребовать от Заказчика уплаты пени в размере 0,1 % (Ноль целых одна десятая процента) от суммы Договора за каждый день просрочки.

7.3 В случае нарушения Исполнителем сроков выполнения обязательств по Договору, Исполнитель выплачивает Заказчику пени в размере 0,1 % (Ноль целых одна десятая процента) от стоимости неисполненного обязательства за каждый день просрочки.

7.4 Если окажется, что какое-либо из заверений и гарантий (включая выявление несоответствия одного/нескольких параметров/характеристик программного обеспечения), данных Исполнителем в рамках настоящего Договора, не соответствует действительности, Заказчик вправе отказаться от исполнения Договора в одностороннем порядке и требовать от Исполнителя возмещения стоимости Договора в сумме, указанной в п. 2.1 Договора, понесенных Заказчиком убытков в полном размере, а также требовать уплаты штрафа в размере 0,1% от суммы, указанной в п. 2.1 Договора.

7.5 Исполнитель вправе досрочно исполнить обязательства по Договору с согласия Заказчика. Согласие Заказчика оформляется официальным письмом.

7.6 В случае досрочного исполнения Исполнителем обязательств по настоящему Договору Заказчик обязан принять Лицензии, Услуги в соответствии с пп. 3.4, 3.9 Договора и оплатить в соответствии с п. 2.3 Договора.

## **8. Обстоятельства непреодолимой силы.**

8.1 Ни одна из Сторон не несет ответственности перед другой Стороной за полное или частичное неисполнение или ненадлежащее исполнение обязательств по Договору, обусловленное действием обстоятельств непреодолимой силы, то есть чрезвычайных ситуаций и непредотвратимых при данных условиях обстоятельств, в том числе объявленной или фактической войной, гражданскими волнениями, эпидемиями, блокадами, пожарами, землетрясениями, наводнениями и другими природными стихийными бедствиями, а также изданием актов государственных органов.

8.2 При наступлении обстоятельств непреодолимой силы каждая Сторона должна не позднее 5 (Пяти) рабочих дней с момента наступления таких обстоятельств известить о них в письменном виде другую Сторону. Извещение должно содержать данные о характере обстоятельств, оценку их влияния на возможность исполнения Стороной своих обязательств по данному Договору, а также предполагаемые сроки их действия.

8.3 В случае наступления обстоятельств непреодолимой силы срок выполнения Стороной обязательств по настоящему Договору отодвигается соразмерно времени, в течение которого действуют эти обстоятельства и их последствия.

8.4 Если действие обстоятельств непреодолимой силы продолжается свыше одного месяца, Стороны проводят дополнительные переговоры для выявления приемлемых альтернативных способов исполнения настоящего Договора либо настоящий Договор подлежит расторжению в установленном порядке.

## **9. Конфиденциальность.**

9.1 Интеллектуальная система учета электроэнергии и автоматизированная система коммерческого учета электроэнергии являются объектом значимой критической



информационной инфраструктуры Российской Федерации, принадлежащим ПАО «Самараэнерго» на законном основании.

9.2 Исполнитель информирован об уголовной ответственности за неправомерное воздействие на значимую критическую информационную инфраструктуру Российской Федерации.

9.3 Стороны обязуются осуществлять передачу и использовать конфиденциальную информацию в соответствии с требованиями, изложенными в Соглашении о конфиденциальности (Приложение № 6 к Договору).

9.4 Дистанционное или удаленное подключение к информационной инфраструктуре Заказчика должно производиться только через VPN туннель.

9.5 Задействованные сетевые порты, сетевые адреса, используемое программное обеспечение, в том числе версии, конфигурация и настройки используемого оборудования в информационной инфраструктуре ПАО «Самараэнерго», а также аутентификационные и идентификационные данные для доступа к информационной инфраструктуре, ПУ, УСПД и другому оборудованию Заказчика, являются конфиденциальными данными.

9.6 Исполнитель должен обеспечить выполнение требований по обеспечению информационной безопасности и защиты интересов ПАО «Самараэнерго» при использовании Исполнителями информационных активов ПАО «Самараэнерго» в соответствии с Регламентом информационной безопасности для подрядчиков/исполнителей (Приложение № 7 к Договору).

9.7 Доступ к конфиденциальной информации, переданной Исполнителю, должен быть ограничен и контролироваться Исполнителем.

9.8 Для получения физического доступа на территорию Заказчика и удаленного доступа к информационной инфраструктуре Заказчика, Исполнитель должен направить на согласование Заказчику запрос по форме в полном соответствии условиям Приложения № 4 и Приложения № 5 к настоящему Договору

9.9 Заявления для печати или иные публичные заявления Исполнителя, связанные с условиями настоящего Договора либо в связи с его исполнением, требуют предварительного письменного согласия Заказчика

9.10 Стороны в течение срока действия настоящего Договора, а также в течение 3 (Трёх) лет по окончании его действия, обязуются обеспечить конфиденциальность условий Договора, а также любой иной информации и данных, получаемых друг от друга в связи с исполнением настоящего Договора (в том числе персональных данных), за исключением информации и данных, являющихся общедоступными (далее – конфиденциальная информация). Каждая из Сторон обязуется не разглашать конфиденциальную информацию третьим лицам без получения предварительного письменного согласия Стороны, являющейся владельцем конфиденциальной информации.

9.11 Стороны обязуются принимать все разумные меры для защиты конфиденциальной информации друг друга от несанкционированного доступа третьих лиц, в том числе:

9.11.1 Хранить конфиденциальную информацию исключительно в предназначенных для этого местах, исключая доступ к ней третьих лиц;

9.11.2 Ограничивать доступ к конфиденциальной информации, в том числе для сотрудников, не имеющих служебной необходимости в ознакомлении с данной информацией.



9.12 Стороны гарантируют полное соблюдение всех условий обработки, хранения и использования полученных персональных данных, согласно ФЗ «О персональных данных» № 152-ФЗ от 27.07.2006.

9.13 Стороны обязаны незамедлительно сообщить друг другу о допущенных ими либо ставшим им известным фактах разглашения или угрозы разглашения, незаконном получении или незаконном использовании конфиденциальной информации третьими лицами.

9.14 Стороны не вправе в одностороннем порядке прекращать охрану конфиденциальной информации, предусмотренной настоящим Договором, в том числе в случае своей реорганизации или ликвидации в соответствии с гражданским законодательством.

9.15 Под разглашением конфиденциальной информации в рамках настоящего Договора понимается действие или бездействие одной из Сторон договора, в результате которого конфиденциальная информация становится известной третьим лицам в отсутствие согласия на это владельца конфиденциальной информации. При этом форма разглашения конфиденциальной информации третьим лицам (устная, письменная, с использованием технических средств и др.) не имеет значения.

9.16 Не является нарушением конфиденциальности предоставление конфиденциальной информации по законному требованию правоохранительных и иных уполномоченных государственных органов и должностных лиц в случаях и в порядке, предусмотренных применимым законодательством, а также предоставление Исполнителем конфиденциальной информации третьим лицам в целях подтверждения опыта и квалификации Исполнителя для участия в закупочных процедурах, не противоречащих законодательству Российской Федерации.

9.17 В случае раскрытия конфиденциальной информации указанным органам и/или лицам Сторона, раскрывшая конфиденциальную информацию, письменно уведомляет владельца конфиденциальной информации о факте предоставления такой информации, ее содержании и органе, которому предоставлена конфиденциальная информация, не позднее двух рабочих дней с момента раскрытия конфиденциальной информации.

9.18 Стороны вправе передавать информацию о факте заключения настоящего Договора и о его предмете партнерам, клиентам и иным лицам.

9.19 В целях защиты персональных данных, а также обеспечения конфиденциальности информации Заказчика, проходящих обработку в автоматизированных системах Заказчика, включая автоматизированные рабочие места, в том числе персональные компьютеры, серверы и системы хранения данных, включая виртуальные и программно-определяемые, любые носители информации не передаются Заказчиком Исполнителю, в том числе в порядке замены носителей информации во исполнение гарантийных обязательств Исполнителем.

9.20 В случае неисполнения Сторонами обязательств, предусмотренных настоящим разделом, Сторона, допустившее такое нарушение, обязуется возместить причиненный этим реальный, документально подтвержденный ущерб в течение 10 (Десяти) рабочих дней после получения соответствующего письменного требования Стороны, считающей себя пострадавшей.

## **10. Условие Договора о порядке уступки требования по денежному обязательству.**

10.1 Заключение договора, предусматривающего уступку права требования по денежному обязательству (в том числе договору факторинга), возможно только по предварительному письменному согласию Заказчика.



10.2 Заказчик должен быть уведомлен в письменной форме Исполнителем или новым кредитором (в том числе финансовым агентом, фактором) в срок не позднее трех дней с момента заключения договора, предусматривающего уступку права требования по денежному обязательству (в том числе договору факторинга), о заключении такого договора с определением подлежащего исполнению денежного требования, а также указанием наименования нового кредитора (в том числе финансового агента, фактора), которому должен быть произведен платеж, и его банковских реквизитов. При этом, в случае направления уведомления новым кредитором (в том числе финансовым агентом, фактором) к нему должно быть приложено доказательство того, что уступка денежного требования новому кредитору (в том числе финансовому агенту, фактору) действительно имела место (договор, предусматривающий уступку права требования по денежному обязательству (в том числе договору факторинга), или надлежащим образом заверенная его копия или иное надлежащее доказательство). Если новый кредитор (в том числе финансовый агент, фактор) не выполнит эту обязанность, Заказчик вправе произвести по данному требованию платеж Исполнителю, во исполнение своего обязательства перед последним.

10.3 Заказчик при исполнении денежного требования новому кредитору (в том числе финансовому агенту, фактору) вправе предъявить к зачету свои денежные требования, вытекающие из настоящего договора, которые уже имелись ко времени, когда было получено уведомление о заключении договора, предусматривающего уступку права требования по денежному обязательству (в том числе договору факторинга).

10.4 Исполнение денежного требования Заказчиком новому кредитору (в том числе финансовому агенту, фактору) освобождает Заказчика от соответствующего обязательства перед Исполнителем.

## **11. Антикоррупционная оговорка.**

11.1 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 для достижения иных неправомерных целей.

11.2 При исполнении своих обязательств по настоящему Договору Стороны, их аффилированные лица, работники или посредники не осуществляют действия, квалифицируемые применимым для целей настоящего Договора законодательством как дача/получение взятки, коммерческий подкуп, а также иные действия, нарушающие требования применимого законодательства и международных актов о противодействии коррупции.

11.3 В случае возникновения у Стороны подозрений, что произошло или может произойти нарушение каких-либо положений п.п. 11.1 и 11.2 настоящего Договора, соответствующая Сторона обязуется уведомить об этом другую Сторону в письменной форме. В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений п.п. 11.1 и 11.2 настоящего Договора другой Стороной, ее аффилированными лицами, работниками или посредниками.

11.4 Сторона, получившая уведомление о нарушении каких-либо положений п.п. 11.1 и 11.2 настоящего Договора, обязана рассмотреть уведомление и сообщить другой Стороне



об итогах его рассмотрения в течение 10 (десяти) рабочих дней с даты получения письменного уведомления.

11.5 Стороны гарантируют осуществление надлежащего разбирательства по фактам нарушения положений п.п. 11.1 и 11.2 настоящего Договора с соблюдением принципов конфиденциальности и применение эффективных мер по предотвращению возможных конфликтных ситуаций. Стороны гарантируют отсутствие негативных последствий как для уведомившей Стороны в целом, так и для конкретных работников уведомившей Стороны, сообщивших о факте нарушений.

11.6 В случае подтверждения факта нарушения одной Стороной положений п.п. 11.1 и 11.2 настоящего Договора и/или неполучения другой Стороной информации об итогах рассмотрения уведомления о нарушении в соответствии с п. 11.3 настоящего Договора, другая Сторона имеет право расторгнуть настоящий Договор в одностороннем внесудебном порядке путем направления письменного уведомления не позднее чем за 14 (четырнадцать) календарных дней до даты прекращения действия настоящего Договора.

## **12. Срок действия договора.**

12.1 Настоящий Договор вступает в силу с момента его подписания обеими Сторонами и действует до 31 декабря 2025 года, но в любом случае до полного выполнения Сторонами своих обязательств по нему.

## **13. Общие положения.**

13.1 Настоящий Договор подписан обеими Сторонами на русском языке в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой Стороны.

13.2 Все изменения и дополнения к настоящему Договору имеют силу в том случае, если они подписаны уполномоченными представителями Сторон. Соответствующие дополнительные соглашения Сторон являются неотъемлемой частью Договора.

13.3 Если любое положение настоящего Договора будет сочтено противоречащим любому приложению к настоящему Договору, превалирующими будут являться положения приложений к настоящему Договору.

13.4 Все споры, которые могут возникнуть из Договора или в связи с ним, Стороны будут стараться разрешить путем переговоров. При невозможности урегулировать спорные вопросы в течение десяти рабочих дней они будут подлежать разрешению в Арбитражном суде Самарской области.

13.5 Любая Сторона обязана в 10 (Десяти) дневный срок уведомлять другую Сторону об изменении своего наименования, адреса и реквизитов, а также реорганизации, начале процедуры банкротства или ликвидации в соответствии с нормами ГК РФ.

13.6 К настоящему Договору прилагаются и являются неотъемлемой его частью:

13.6.1 Приложение № 1. Техническое задание.

13.6.2 Приложение № 2. Спецификация.

13.6.3 Приложение № 3. Проектная документация.

13.6.4 Приложение № 4. Порядок оформления запроса физического доступа на территорию ПАО «Самараэнерго».

13.6.5 Приложение № 5. Порядок оформления запроса предоставления удалённого доступа (компьютерного) к сетевой инфраструктуре ПАО «Самараэнерго».

13.6.6 Приложение № 6. Соглашение о конфиденциальности.

13.6.7 Приложение № 7. Регламент информационной безопасности для подрядчиков/исполнителей.



#### 14. Адреса, реквизиты и подписи Сторон.

##### Заказчик

Наименование полное: Публичное акционерное общество энергетики и электрификации «Самараэнерго»

Наименование сокращенное: ПАО «Самараэнерго»

Адрес полный из ЕГРЮЛ: 443079, область Самарская, город Самара, проезд Георгия Митирева, дом 9

Адрес почтовый для корреспонденции: 443079, Российская Федерация, город Самара, проезд Георгия Митирева, дом 9

Телефон: (8-846) 340-38-63

ИНН 6315222985, КПП 997650001

ОГРН 1026300956131, ОКПО 00102504,

р/с 40702810054400031730

в Поволжском банке ПАО «Сбербанк России»

БИК 043601607

к/с 30101810200000000607

e-mail: [info@samaraenergo.ru](mailto:info@samaraenergo.ru)

##### Исполнитель

Наименование полное: Публичное акционерное общество «Ростелеком»

Наименование сокращенное: ПАО «Ростелеком»

Юридический адрес (местонахождение): 191167, город Санкт-Петербург, вн. тер. г. Муниципальный округ Смольнинское, Синопская набережная, дом 14, литера А

Почтовый адрес: Российская Федерация, 115172, г. Москва, ул. Гончарная, дом 30

Фактический адрес: Российская Федерация, 443010, г. Самара, ул. Красноармейская, 17

ИНН 7707049388 КПП 784201001

КПП по месту нахождения филиала 631543001

ОГРН 1027700198767

ОКПО 17514186

р/с 40822810338000000002

к/с 30101810400000000225

ПАО СБЕРБАНК

БИК 044525225

Тел/факс: (846) 332-10-20, (846) 340-05-10 (факс)

e-mail: [director@volga.rt.ru](mailto:director@volga.rt.ru)

Заместитель генерального директора по техническим вопросам и информационным технологиям



Р.Л. Шуман

м. п.

Заместитель директора филиала - директор по работе с корпоративным и государственным сегментами Самарского филиала ПАО «Ростелеком»



А.Н. Толочная

м. п.







## ТЕХНИЧЕСКОЕ ЗАДАНИЕ

**ПРИОБРЕТЕНИЕ НЕИСКЛЮЧИТЕЛЬНЫХ ПРАВ ИСПОЛЬЗОВАНИЯ  
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ АНАЛИЗА ЗАЩИЩЕННОСТИ  
ИНФОРМАЦИИ И ОКАЗАНИЕ УСЛУГ ПО ВНЕДРЕНИЮ ПРОГРАММНОГО  
ОБЕСПЕЧЕНИЯ СИСТЕМЫ АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ**

САМАРА  
2025





# 1 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

## Термины и определения

№	ТЕРМИН	ОПРЕДЕЛЕНИЕ
1.	Аутентификация	Действия по проверке подлинности субъекта доступа и (или) объекта доступа, а также по проверке принадлежности субъекту доступа и (или) объекту доступа предъявленного идентификатора доступа и аутентификационной информации
2.	Доступность	Состояние информации (информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно
3.	Защищенность	Характеристика системы, отражающая способность системы противостоять рискам, нацеленным на нарушение конфиденциальности, целостности или доступности
4.	Зеркалирование данных	Процесс одновременной записи нескольких взаимозаквивалентных копий данных
5.	Идентификация	Действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.
6.	Информационная система	Система, организующая обработку информации о предметной области и ее хранение
7.	Интегральная уязвимость	Оценка опасности всех уязвимостей ИТ-актива
8.	ИТ-актив	Элемент, вещь или сущность, которые могут использоваться для получения, обработки, хранения и распространения информации (цифровых данных), которая имеет потенциальную или фактическую ценность для организации
9.	Контролируемая зона	Пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.
10.	Модифицируемость	Степень простоты эффективного и рационального изменения продукта или системы без добавления дефектов и снижения качества продукта
11.	Отказоустойчивость	Способность системы, продукта или компонента работать как предназначено, несмотря на наличие дефектов программного обеспечения или аппаратных средств.
12.	Сканирование в режиме черного ящика	Проверка ИТ-актива, при которой не используется знание о внутреннем устройстве (коде) ИТ-актива
13.	Сканирование в режиме белого ящика	Проверка ИТ-актива, при которой используется знание о внутреннем устройстве (коде) ИТ-актива
14.	Угроза	Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб или вред) для организации
15.	Уязвимость	Свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации.
16.	ИТ-инфраструктура	Совокупность компонентов информационных технологий, в том числе аппаратное (системы обработки и хранения данных, оборудование рабочего места, периферия и т.д.), системное программное и инженерное обеспечение, сети, специализированные помещения.
17.	Общество	ПАО «Самараэнерго»
18.	Привилегированный пользователь	Пользователь, обладающий легитимными расширенными полномочиями в работе с корпоративными системами, включая их установку, настройку и обслуживание
19.	Специальные средства защиты информации (СЗИ)	Программные и (или) программно-аппаратные средства, внедряемые в периметре информационной системы с целью обеспечения защиты обрабатываемой информации.
20.	Структурное подразделение ИБ	Структурное подразделение Общества ответственное за обеспечение информационной безопасности объектов Общества.
21.	Структурное подразделение ИТ	Структурное подразделение Общества, ответственное за развитие информационных технологий, предоставление ИТ-сервисов, автоматизации бизнес-процессов.
22.	Структурное подразделение (СП)	Структурное подразделение с самостоятельными функциями, задачами и ответственностью в рамках своей компетенции, определенной Положением о структурном подразделении.



№	ТЕРМИН	ОПРЕДЕЛЕНИЕ
23.	Целевой ресурс, Целевая система	Ресурс сети Заказчика (адрес протокола IP – средство вычислительной техники, устройство сети передачи данных и т.д.), к которому требуется обеспечить доступ привилегированных пользователей

### Сокращения

№	СОКРАЩЕНИЕ	ОПРЕДЕЛЕНИЕ
1.	AD	Active Directory
2.	DNS	Domain name system
3.	FTP	File transfer protocol
4.	HTTP	Hypertext transfer protocol
5.	IAM	Identity and Access Management
6.	LDAP	Lightweight Directory Access Protocol
7.	OSI	Open Systems Interconnection
8.	POP3	Post Office Protocol Version 3
9.	RDP	Remote desktop protocol
10.	SMB	Server Message Block
11.	SMTP	Simple mail transport protocol
12.	SNMP	Simple network management protocol
13.	SSO	Single Sign-on
14.	SQL	Structured query language
15.	SSH	Secure Shell
16.	TCP	Transmission Control Protocol
17.	UDP	User Datagram Protocol
18.	VNC	Virtual Network Computing
19.	IP	Internet Protocol
20.	GUI	Graphical User Interface
21.	NTP	Network Time Protocol
22.	RPO	(англ. Recovery point objective) - Максимальное окно потери данных в результате инцидента
23.	RTO	(англ. Recovery time objective) - период времени, установленный для возобновления функционирования Системы после инцидента с учетом возможности предоставления доступа пользователям.
24.	SSL	(англ. Secure Sockets Layer — уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь, использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.



№	СОКРАЩЕНИЕ	ОПРЕДЕЛЕНИЕ
25.	URL	Uniform Resource Locator
26.	VLAN	Virtual Local Area Network
27.	АРМ	Автоматизированное рабочее место
28.	АО	Акционерное общество
29.	АСКУЭ	Автоматизированная система коммерческого учета электроэнергии
30.	БД	База данных
31.	ВМ	Виртуальная машина
32.	ИБ	Информационная безопасность
33.	КИИ	Критическая информационная инфраструктура
34.	НКЦКИ	Национальный координационный центр по компьютерным инцидентам
35.	НСД	Несанкционированный доступ
36.	ОЭ	Опытная эксплуатация
37.	ЗОКИИ	Значимый объект критической информационной инфраструктуры
38.	ПАЗИ	Подсистема анализа защищенности информации
39.	ПО	Программное обеспечение
40.	ПиМИ	Программа и методика испытаний
41.	КСОИБ	Комплексная система обеспечения информационной безопасности
42.	СЗИ	Средство защиты информации
43.	СКЗИ	Средство криптографической защиты информации.
44.	СУ	Система управления
45.	СУБД	Система управления базами данных
46.	ТЗ	Техническое задание
47.	ФСТЭК	Федеральная служба по техническому и экспортному контролю
48.	ФЗ	Федеральный закон

## 2 ПРЕДМЕТ ЗАКУПКИ

Приобретение неисключительных прав использования программного обеспечения системы анализа защищенности информации и оказание услуг по внедрению программного обеспечения системы анализа защищенности информации для нужд ПАО «Самараэнерго».

## 3 ЦЕЛИ И РЕШАЕМЫЕ ЗАДАЧИ

Целью закупки является создание системы анализа защищенности информации для обеспечения защиты ИТ-инфраструктуры Общества, реализация мер по обеспечению информационной безопасности в рамках создания комплексной системы по обеспечению



защиты ЗОКИИ Общества в соответствии с требованиями законодательства Российской Федерации, в том числе выполнение требований Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», обеспечение соответствия создаваемой инфраструктуры для ПО «Телескоп+» требованиям законодательства РФ в области обеспечения безопасности объектов критической информационной инфраструктуры, а также нейтрализации угроз информационной безопасности, реализация которых может привести к нарушению штатного режима функционирования ИС и управляемого (контролируемого) процесса, локализацию и минимизацию последствий от возможной реализации угроз безопасности информации, согласно пояснительной записки на создание КСОИБ ЗОКИИ Общества (02409271.26.20.40.140.139.П2) (Приложение № 3 к Договору).

Создаваемая в рамках данного технического задания система анализа защищенности информации является одной из подсистем комплексной системы обеспечения информационной безопасности ЗОКИИ Общества – подсистема анализа защищенности информации (далее - ПАЗИ).

Назначением внедряемой ПАЗИ является:

- Сбор данных о сетевых узлах и связях между ними для выявления информации или оборудования, имеющих ценность для Общества и подлежащих защите от угроз информационной безопасности
- Управление уязвимостями ИТ-активов, в том числе:
  - поиск уязвимостей активов в режиме черного и белого ящика
  - контроль устранения выявленных уязвимостей
  - оценка эффективности выполнения контроля защищенности и действий, связанных с устранением нарушений безопасности
- Контроль соблюдения требований политик и стандартов безопасности

Для достижения поставленных целей Исполнителю требуется реализовать следующие задачи:

1. Осуществить передачу Заказчику программного обеспечения и сертифицированного медиа-пака программного обеспечения ПАЗИ, необходимых для реализации проекта и отвечающего требованиям настоящего технического задания.
2. Оказать услуги по внедрению программного обеспечения ПАЗИ в соответствии с требованиями пояснительной записки на создание КСОИБ ЗОКИИ Общества (02409271.26.20.40.140.139.П2) (Приложение № 3 к Договору) и данного технического задания.

#### **4 ПЛАНОВЫЕ СРОКИ НАЧАЛА И ОКОНЧАНИЯ УСЛУГ**

Срок начала оказания услуг: с момента подписания договора.

Срок полного и окончательного выполнения работ/услуг по договору, включая передачу Исполнителем Заказчику всей требуемой условиями договора документации не должен быть позднее 10.12.2025 года.

## **5 МЕСТО ОКАЗАНИЯ УСЛУГ**

Услуги оказываются по адресу размещения серверного оборудования Заказчика: г. Самара, проезд Георгия Митирева, д.9.

## **6 ОБЩИЕ СВЕДЕНИЯ**

Настоящее техническое задание (ТЗ) является документом, определяющим требования и порядок реализации мер по внедрению программного обеспечения системы анализа защищенности информации в значимом объекте критической информационной инфраструктуры «Интеллектуальная система учета электроэнергии и автоматизированная система коммерческого учета электроэнергии (АСКУЭ)» (далее ЗОКИИ).

Реализация мер по обеспечению информационной безопасности выполняется в рамках создания комплексной системы по обеспечению защиты ЗОКИИ (далее КСОИБ) от неправомерного доступа, уничтожения, модификации, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении защищаемой информации в соответствии с законодательством Российской Федерации (далее РФ), в том числе федерального закона Российской Федерации от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

### **6.1 ХАРАКТЕРИСТИКА ОБЪЕКТА ЗАЩИТЫ**

ПАО «Самараэнерго» является значимым объектом критической информационной инфраструктуры. Объекту КИИ ПАО «Самараэнерго», присвоена Категория – II.

В соответствии с адаптированным набором мер по обеспечению безопасности, требованиями технического задания и присвоенной категорией определен состав подсистем КСОИБ, в том числе подсистемы анализа защищенности информации (ПАЗИ).

Работа основных подсистем КСОИБ Общества реализуется с использованием ресурсов комплекса технических средств проекта 02409271.26.20.40.140.138 «Инфраструктура для ПО «Телескоп+» (Приложение № 3 к Договору) и следующих обеспечивающих подсистем:

- серверной инфраструктуры и хранения данных;
- технологической сети передачи данных;
- виртуальной инфраструктуры.

Основные требования и решения ПАЗИ определены в Пояснительной записке на создание КСОИБ (02409271.26.20.40.140.139.П2) (Приложение № 3 к Договору).

Подробное описание объекта защиты приведено в п.2 Пояснительной записки на создание КСОИБ (02409271.26.20.40.140.139.П2) (Приложение № 3 к Договору).

### **6.2 КАТЕГОРИЯ ЗНАЧИМОСТИ ОБЪЕКТА КИИ**

Проектные решения Исполнителя должны обеспечивать соответствие требованиям установленной II категории значимости в соответствии с приложением к Приказу №239 ФСТЭК России от 25.12.2017 г.



### 6.3 ПЕРЕЧЕНЬ ДОКУМЕНТОВ, НА ОСНОВАНИИ КОТОРЫХ ВНЕДРЯЕТСЯ ПАЗИ

Оказание услуг по внедрению ПАЗИ проводятся в соответствии с действующими редакциями следующих законодательных актов, нормативно-распорядительных документов и государственных стандартов:

- федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
- приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановление Правительства РФ от 19 июня 2020 г. № 890 «О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)»;
- указ Президента Российской Федерации от 30.03.2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры»;
- указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
- ГОСТ Р 59793-2021 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

- ГОСТ Р 59795–2021 «Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы»;
- ГОСТ Р 59792-2021 «Информационная технология. Виды испытаний автоматизированных систем»;
- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
- ГОСТ 34.602–2020 «Техническое задание на создание автоматизированной системы»;
- ГОСТ 34.201–2020 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Виды, комплектность и обозначение документов»;
- ГОСТ Р 59853–2021 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
- Отчет об обследовании инфраструктуры ПО «Телескоп+»;
- Проектная документация на создание инфраструктуры для ПО «Телескоп+».

## 6.4 РАЗДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ

Необходимое для реализации требований данного технического задания аппаратное и программное обеспечение, в том числе операционные системы предоставляются Заказчиком в составе:

- Виртуальный сервер – 1 шт.
- ОС Astra Linux Special Edition, ФСТЭК («Воронеж», «Смоленск») – 1 шт.
- ПО ПАЗИ (поставляемое в рамках данного договора) – 1 шт.

Заказчик обеспечивает предоставление доступа к виртуальному серверу для развертывания ПАЗИ согласно Пояснительной записки (02409271.26.20.40.140.138.ПЗ) (Приложение № 3 к Договору).

Для нормальной эксплуатации разрабатываемой системы Заказчиком обеспечивается бесперебойное питание компонентов ПАЗИ.

Заказчик обеспечивает подготовку смежных подсистем согласно Пояснительной записке (02409271.26.20.40.140.138.ПЗ) (Приложение № 3 к Договору) и разработанной Исполнителем документации.

Заказчик обеспечивает подготовку на АРМ и Серверах инфраструктуры ЗОКИИ технических учетных записей, которые включаются на период проведения сканирования.

Заказчик обеспечивает наличие и работоспособность скомпонованных и настроенных должным образом межсетевых экранов для защиты ПАЗИ при передаче информации по каналам связи из одной ИС в другую.

Заказчик обеспечивает наличие и работоспособность защищенных каналов связи, защищенных волоконно-оптических линий связи либо наличие, работоспособность и функционирование должным образом средств криптографической защиты информации в случае использования каналов связи, выходящих за пределы контролируемой зоны.



## 7 ОБЩИЕ ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ И ОКАЗАНИЮ УСЛУГ

### 7.1 ТРЕБОВАНИЯ К ПОСТАВЛЯЕМОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

Программное обеспечение должно быть включено в реестр российского программного обеспечения или реестр евразийского программного обеспечения.

Согласно приказу ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» программное обеспечение ПАЗИ должно быть сертифицировано на соответствие требованиям по безопасности информации средств защиты информации не ниже 5 класса защиты, и соответствовать 5 или более высокому уровню доверия.

В случае отсутствия действующего сертификата ФСТЭК допускается предоставление сертификата ФСТЭК с истекшим сроком действия, при соблюдении положений Приказа ФСТЭК России от 03.04.2018 N 55 (ред. от 19.09.2022) «Об утверждении Положения о системе сертификации средств защиты информации», а именно: серийно производимое средство защиты информации произведено в период срока действия сертификата соответствия на его серийное производство, соответствует требованиям по безопасности информации и изготовитель осуществляет его техническую поддержку.

Используемое при разработке/внедрении программное обеспечение и библиотеки должны иметь широкое распространение, быть общедоступными, использоваться в промышленных масштабах.

Состав используемого ПО ПАЗИ должен быть определен на этапе подготовки технического решения и соответствовать требованиям законодательства РФ, в части требований предъявляемым к ПО используемому на объектах ЗОКИИ.

Установка системы в целом, как и установка отдельных частей системы, не должна предъявлять дополнительных требований к покупке лицензий на программное обеспечение сторонних производителей, кроме программного и аппаратного обеспечения, входящего в состав информационной системы и перечисленного в настоящем документе.

Лицензии на право использования программного обеспечения системы контроля привилегированного доступа должны принадлежать ПАО «Самараэнерго».

Передача Лицензий осуществляется по адресу местонахождения Заказчика в срок не позднее 15 календарных дней с момента заключения договора.

В рамках создания ПАЗИ в Обществе Исполнитель должен осуществить поставку лицензий на ПО ПАЗИ с техническими характеристиками, приведенными в Таблице №1.

Таблица № 1

№ п/п	Наименование характеристики	Значение характеристики
1.	Лицензия на программное обеспечение системы анализа защищенности информации для выявления уязвимостей и проверки соответствия стандартам не менее 250 активов, обновления в течение 1 (одного) года 1 шт.	-



	<i>(PT-MPSIEM-VM-HCC-AIO-250 Программное обеспечение MaxPatrol Security Information and Event Management. Конфигурация MaxPatrol VM HCC All-In-One для выявления уязвимостей и проверки соответствия стандартам не более 250 активов, обновления в течении 1 (одного) года)</i>	
1.1.	Максимальное количество сканируемых активов	250
1.2.	Срок действия лицензии	Бессрочно
1.3.	Срок предоставления обновлений	Один год
1.4.	Обеспечение возможности сбора данных на основе задач, использующих шаблоны (профили) сбора данных; (однократно и по расписанию)	Да
1.5.	Обеспечение возможности создания, изменения, удаления, запуска и приостановки задач на сбор данных	Да
1.6.	Поддержка списка исключений – перечня сетевых узлов, на которых запрещено выполнение задач на сбор данных	Да
1.7.	Поддержка настройки запрещенного времени для выполнения задач на сбор данных: на указанный интервал времени выполнение задачи должно прерываться	Да
1.8.	Поддержка возможности запуска задач на основе расписания, задаваемого через графический веб-интерфейс или в формате строки Crontab	Да
1.9.	Поддержка возможности создания задач для нескольких выбранных модулей сбора данных (с автоматическим созданием и распределением подзадач)	Да
1.10.	Поддержка возможности просмотра перечня подзадач для конкретной задачи на сбор данных	Да
1.11.	Поддержка возможности сортировки и поиска задач на сбор данных по их атрибутам	Да
1.12.	Обеспечение возможности создания, изменения, удаления шаблонов (профили) сбора данных, определяющие протоколы и способы сбора данных от источников данных	Да
1.13.	Поддержка возможности экспорта и импорта результатов выполнения задач на сбор данных	Да
1.14.	Поддержка возможности поиска профилей сбора данных	Да
1.15.	Обеспечение возможности создания, изменения, удаления учетных записей, необходимых для авторизации на источниках данных	Да
1.16.	Обеспечение возможности экспорта и импорта профилей сбора данных в файл	Да
1.17.	Обеспечение метода добавления активов путем сканирования сети с выявлением и идентификацией активов, включенных и подключенных к локальным вычислительным сетям с использованием стека TCP/IP	Да
1.18.	Обеспечение добавления активов в ручном режиме	Да
1.19.	Обеспечение добавления активов путем импорта активов из CSV-файла	Да
1.20.	Обеспечение сбора при сканировании сведений об ИТ-активах (сетевых узлах ИС) в области, заданной пользователем по IP адресам (подсетям), именам или внутрисистемным идентификаторам активов с возможностью ограничения или выбора числа портов и протоколов транспортного уровня, используемых при сканировании	Да
1.21.	Обеспечение сбора при сканировании инвентаризационной информации активов (идентификация доступных сетевых служб и ПО), в том числе наименования и версии ОС семейства Microsoft Windows, сетевых служб, использующих транспортные протоколы TCP и UDP	Да
1.22.	Обеспечение сбора при сканировании сбор сведений об уязвимых учетных данных (слабых парах «логин – пароль»), получаемых путем подбора с использованием справочников по протоколам: - электронной почты – SMTP, POP3; - файловых служб – FTP; - удаленного управления – RDP, SSH, Telnet, SNMP, VNC, Radmin, Symantec PCAnywhere, NetBIOS; - баз данных – Microsoft SQL, Oracle DB, Sybase, DB2, MySQL, PostgreSQL; - бизнес-приложений – SAP DIAG, SAP RFC; - сред виртуализации – VMware vSphere; - IP-телефонии – SIP	Да
1.23.	Поддержка справочников для сетевого сканирования: - базовые заполненные справочники с парами «логин – пароль»;	Да



	- пользовательские справочники для хранения пар «логин – пароль», справочники с логинами, справочники с паролями	
1.24.	Поддержка возможности создания, изменения или удаления пользовательских справочников	Да
1.25.	Поддержка подключения к выбранным ИТ-активам по IP-адресам (подсетям), FQDN-именам или иным идентификаторам ИТ-активов	Да
1.26.	Поддержка выбора способов (протоколов) подключения к ИТ-активам и определения учетных записей, используемых для аутентификации	Да
1.27.	Поддержка механизма проверки доступности ИТ-активов для выполнения задач на сбор данных, в том числе поддержка проверки учетной записи, используемой при проверке доступности	Да
1.28.	Обеспечение сбора инвентаризационной и конфигурационной информации путем сканирования ИТ-активов: - идентификационных данных об ИТ-активах (IP-адрес, FQDN и другие); - данных о составе аппаратного обеспечения (материнская плата, центральный процессор, сетевая карта и другие); - данных о составе программного обеспечения (BIOS, ОС, общесистемное ПО и другие); - данных о настройках ОС семейства Windows (локальные и доменные политики); - данных о запущенных службах и задачах планировщика ОС.	Да
1.29.	Поддержка сканирования узлов инфраструктуры (активов) методами белого и черного ящика.	Да
1.30.	Обеспечение автоматического выявления уязвимостей в соответствии с экспертной базой знаний на ИТ-активах с наличием информации достаточной для расчета уязвимостей	Да
1.31.	Обеспечение выявления уязвимостей в пакетах программ, вложенных в контейнеры, основанные на ОС семейства Linux, в том числе Debian и Ubuntu	Да
1.32.	Обеспечение модулями сбора данных, размещенными на технических средствах под управлением ОС семейства Linux возможности создания, изменения, удаления, запуска и приостановки задач поиска уязвимостей в веб-приложениях	Да
1.33.	Обеспечение отображения сведений об уязвимостях в виде карточки уязвимости, связанной с карточкой ИТ-актива	Да
1.34.	Отображение времени последнего сканирования ИТ-актива на наличие уязвимостей	Да
1.35.	Обеспечение управления списком ИТ-активов, включая: - поиск ИТ-активов по их атрибутам; - группировку ИТ-активов; - построение иерархии групп ИТ-активов; - поиск групп ИТ-активов по названию	Да
1.36.	Поддержка группировки ИТ-активов в статические группы, членство ИТ-актива в которых определяется пользователем	Да
1.37.	Поддержка группировки ИТ-активов в динамические группы, членство в которых определяется ПО ПАЗИ автоматически на основе информации об ИТ-активе (IP-адреса, ОС, прочих характеристик)	Да
1.38.	Обеспечение контроля ключевых показателей процесса управления ИТ-активами путем реализации настраиваемых политик и (или) правил, включая: - активацию или деактивацию политики и (или) правила; - добавление, изменение или удаление политики и (или) правила	Да
1.39.	Поддержка реализации политики и (или) правила определения и (или) изменения сроков актуальности и устаревания данных об активе	Да
1.40.	Поддержка реализации политики и (или) правила определения перечня активов, в отношении которых действует политика и (или) правило	Да
1.41.	Поддержка реализации политики и (или) правила присвоения значимости ИТ-активам	Да
1.42.	Обеспечение выполнения над ИТ-активом действий, описанных в политике и (или) правиле (при ИТ-активации политики и (или) правила)	Да
1.43.	Обеспечение возвращения состояния ИТ-актива в исходное при деактивации политики и (или) правила	Да
1.44.	Обеспечение отображения собранной конфигурационной информации об активе в виде карточки ИТ-актива	Да
1.45.	Обеспечение автоматического изменения инвентаризационной и конфигурационной информации об ИТ-активах в результате выполнения задач на сбор данных	Да



1.46.	Обеспечение управления карточками активов, включая: - ручное добавление, изменение (в том числе добавление пользовательских полей описания ИТ-актива) или удаление карточки ИТ-актива; - отображение даты и времени последнего обновления информации об активе; - задание уровня значимости ИТ-актива; - задание статусов (сроков) актуальности данных	Да
1.47.	Обеспечение поддержки следующих механизмов фильтрации и сортировки карточек активов: - сортировка и фильтрация перечня активов по заданному набору атрибутов и их значениям; - быстрое создание группы фильтрации путем одиночного нажатия левой клавиши мыши на значение одного из основных атрибутов ИТ-актива; - возможность отображения активов, удовлетворяющих условиям заданного фильтра	Да
1.48.	Обеспечение ведения истории изменения карточки ИТ-актива с отображением истории изменения карточек активов с возможностью: - просмотра состояния ИТ-актива на заданный момент времени или за указанный период; - сравнения конфигураций ИТ-актива в два различных момента времени	Да
1.49.	Обеспечение поддержки работы с топологией сети, включая: - построение и визуализацию топологии сети на уровне L3 модели OSI на основе собранной ПО ПАЗИ информации об ИТ-активах; - возможность проверки сетевой доступности между ИТ-активами на основе собранной ПО ПАЗИ информации об ИТ-активах; - возможность отображения активов, удовлетворяющих условиям заданного фильтра	Да
1.50.	Обеспечение представления сведений об уязвимостях в соответствии с таксономией (принципами классификации и систематизации) стандартов CVSSv2 и CVSSv3	Да
1.51.	Обеспечение расчета уровня критичности выявленных уязвимостей в соответствии с методическим документом ФСТЭК России от 28 октября 2022 г. «Методика оценки уровня критичности уязвимостей программных и программно-аппаратных средств»	Да
1.52.	Поддержка возможности сортировки программного обеспечения согласно алгоритму принятия решений для процесса управления обновлениями программного обеспечения, установленного Бюллетенями Национального координационного центра по компьютерным инцидентам (НКЦКИ)	Да
1.53.	Обеспечение наличия ссылок на публичные базы данных, в которых описаны уязвимости того же типа, что и обнаруженные	Да
1.54.	Обеспечение отображения оценки обнаруженных уязвимостей по признакам: - последняя добавленная; - трендовая; - на важном активе; - имеющая известный эксплойт; - доступная для удаленного использования	Да
1.55.	Обеспечение оценки интегральной уязвимости для ИТ-актива	Да
1.56.	Поддержка ручного управления карточками уязвимостей	Да
1.57.	Обеспечение обработки уязвимостей на основе политик и (или) правил: - для контроля устранения уязвимостей: 1) определение действий по отношению к уязвимостям в результате применения правила; 2) определение статуса, который получает уязвимость при выполнении правила; 3) определение перечня уязвимостей, в отношении которых действует правило; 4) определение перечня активов, в отношении которых действует правило. - для пометки критически важных уязвимостей: 1) присвоение уникальной метки, по которой легко выявить помеченный актив; 2) определение перечня уязвимостей, в отношении которых действует правило; 3) определение перечня активов, в отношении которых действует правило	Да
1.58.	Обеспечение контроля ключевых показателей процесса управления уязвимостями путем реализации настраиваемых политик и (или) правил, включая: - активацию и (или) деактивацию политики и (или) правила;	Да



	- добавление и (или) изменение и (или) удаление политики и (или) правила	
1.59.	Поддержка операций над сведениями об уязвимостях: - выделение важных (критических) уязвимостей; - контроль выполнения работ по устранению уязвимостей; - градация уязвимостей, в том числе выявление трендовых уязвимостей, то есть уязвимостей, которые активно используются в атаках злоумышленников в актуальный период времени (при условии постоянных обновлений базы знаний)	Да
1.60.	Поддержка операций управления обработкой уязвимостей: - поиск и сортировка уязвимостей по их атрибутам; - создание и (или) удаление информации (меток) к уязвимостям; - демонстрация карточек уязвимостей, содержащих справочную информацию в развернутом виде; - изменение статуса уязвимости; - контроль устранения уязвимостей; - проведение массовых операций над уязвимостями	Да
1.61.	Поддержка поиска по активам и уязвимостям с применением технологии искусственного интеллекта на русском и английском языках	Да
1.62.	Обеспечение ведения истории изменения уязвимостей с привязкой к конкретному активу, с отображением: - наличия уязвимости; - статуса уязвимости на заданный момент времени	Да
1.63.	Наличие предустановленного набора стандартов	Да
1.64.	Обеспечение проверки соответствия и принятие решений о соответствии текущих параметров программных и программно-технических средств (ИТ-активов) требованиям предустановленных в ПО ПАЗИ технических стандартов	Да
1.65.	Поддержка возможности импорта пользовательских стандартов в формате YAML	Да
1.66.	Поддержка возможности импорта пользовательских требований	Да
1.67.	Поддержка механизма валидации импортируемых требований	Да
1.68.	Обеспечение валидации требований, существующих в ПО ПАЗИ (при внесении изменений, влияющих на работу требования)	Да
1.69.	Обеспечение отображения критичности требований в стандарте (по уровню опасности)	Да
1.70.	Поддержка возможности установки пользовательских меток на конкретные требования	Да
1.71.	Поддержка возможности указания для каждого импортируемого стандарта следующих параметров: - идентификатор стандарта; - отображаемое имя стандарта; - текстовое описание стандарта; - название регламентирующего документа, на основании которого создан стандарт; - параметры привязки узлов ИТ-актива к требованию; - требования, входящие в стандарт; - новые значения параметров требований (при необходимости)	Да
1.72.	Поддержка возможности создания политик и (или) правил проверки соответствия стандартам	Да
1.73.	Поддержка возможности присвоения статусов ИТ-активам, не соответствующим стандартам	Да
1.74.	Поддержка возможности создания политик и (или) правил устранения несоответствия ИТ-актива стандарту	Да
1.75.	Поддержка возможности просмотра оценки соответствия ИТ-актива стандарту (по результатам его проверки правилом проверки соответствия)	Да
1.76.	Обеспечение хранения данных, содержащих выявленные в различные моменты времени сведения об ИТ-активах, в том числе IP-адреса, доменные имена и другие данные	Да
1.77.	Возможность хранения данных на внешних системах хранения	Да
1.78.	Обеспечение хранения сведений о выявленных уязвимостях	Да



1.79.	Обеспечение хранения данных, используемых при проверке на уязвимости методом черного ящика	Да
1.80.	Поддержка возможности периодического автоматического удаления промежуточных (неактуальных) данных об активах	Да
1.81.	Обеспечение реализации ролевой модели управления доступом к компонентам и функциям ПО ПАЗИ	Да
1.82.	Обеспечение идентификации и аутентификации пользователей ПО ПАЗИ на основе учетных записей	Да
1.83.	Предоставление графического веб-интерфейса, обеспечивающего: - доступ к функциям на основе прав пользователей или их ролей; - информирование уполномоченных пользователей о состоянии всех компонентов, входящих в состав ПО ПАЗИ, и работоспособности ПО ПАЗИ; - отображение результатов работы ПО ПАЗИ в виде текстовых и графических данных	Да
1.84.	Обеспечение возможности управления учетными записями пользователей ПО ПАЗИ: - созданием, изменением, блокированием или удалением учетных записей; - назначением и изменением логинов и паролей; - назначением ролей; - выбором методов аутентификации (локальная база или LDAP-аутентификация)	Да
1.85.	Обеспечение отображения результатов самодиагностики работы компонентов ПО ПАЗИ и оповещения пользователя о неисправностях	Да
1.86.	Обеспечение визуализации статистических данных о результатах функционирования Системы с помощью панелей мониторинга, а также отображения оперативных данных об ИТ-активах и работоспособности Системы в виде графиков, диаграмм и таблиц, закрепляемых за отдельными виджетами	Да
1.87.	Обеспечение наличия предустановленных панелей мониторинга	Да
1.88.	Обеспечение возможности создания пользовательских панелей мониторинга	Да
1.89.	Обеспечение наличия предустановленных виджетов по ИТ активам, отображающим: - количество активов; - значимость активов; - актуальность данных об ИТ-активах	Да
1.90.	Обеспечение наличия предустановленного виджета с изменениями статусов по уязвимостям повышенного уровня опасности (критический и высокий), произошедшими в течение семи дней	Да
1.91.	Обеспечение возможности настройки, построения, отправки и экспорта отчетов	Да
1.92.	Обеспечение наличия предустановленных форм отчетов	Да
1.93.	Поддержка возможности создания пользовательских форм отчетов с помощью конструктора отчетов, позволяющего: 1) задать последовательность объектов отчета (текста, изображений, актуальной информации из виджетов); 2) задать тип визуализации данных (диаграммы, графики, гистограммы); 3) настроить внешний вид отчета (колоннотитулы, легенду, подписи к объектам отчета).	Да
1.94.	Поддержка возможности выпуска отчетов вручную или по расписанию, в том числе с отправкой на заданный адрес электронной почты	Да
1.95.	Поддержка возможности экспорта отчетов в один из следующих форматов: JSON, PDF, CSV, XML, XLSX	Да
1.96.	Обеспечение наличия активных ссылок на внешние источники сведений об уязвимостях при экспорте отчетов в формате XLSX	Да
1.97.	Обеспечение журналирования действий пользователей: - с ИТ-активами в интерфейсе ПО ПАЗИ; - в части управления сбором данных; - в части управления контентом базы знаний; - в части управления ПО ПАЗИ; - во всех случаях авторизации пользователей	Да
1.98.	Обеспечение уведомления уполномоченных пользователей об изменении статусов основных системных сущностей (активов, задач на сбор данных, состояния системы) с их отправкой на электронную почту или по POST-запросу	Да



1.99.	Обеспечение автоматической проверки актуальности правил и (или) политик проверки соответствия стандартам	Да
1.100.	Обеспечение отображения статуса недействующих правил и (или) политик: в связи с устареванием или в случае, если в правилах и (или) политике появились сообщения об ошибках	Да
1.101.	Обеспечение отображения очереди построения отчетов	Да
1.102.	Поддержка возможности управления очередью построения отчетов	Да
1.103.	Обеспечение возможности автоматизированного (запускаемого в ручном режиме) обновления программного обеспечения	Да
1.104.	Поддержка пакетной доставки уязвимостей и баз уязвимостей, в том числе при установке со съемных носителей информации	Да
1.105.	Лицензия на ПО ПАЗИ должна включать техническую поддержку на период обновлений (1 год)	Да
1.106.	Наличие сертификата ФСТЭК на ПО ПАЗИ на соответствие требованиям по безопасности информации средств защиты информации не ниже 5 класса защиты и 5 или более высокому уровню доверия на поставляемое ПО ПАЗИ, входящее в комплект поставки	№ 4980
1.107.	Прием обращений на портале технической поддержки	Да
1.108.	Диагностика сбоев и предоставление рекомендаций по их устранению	Да
1.109.	График приема и обработки обращений – с 9:00 до 18:00 по московскому времени кроме субботы, воскресенья, официальных нерабочих праздничных дней в Российской Федерации	Да
1.110.	Наличие в комплекте поставки программного обеспечения установочного комплекта на машинном носителе содержащего: – файлы инсталляционного комплекта входящего в комплект поставки сертифицированной версии; – формуляр с требованиями по эксплуатации, приложения к формуляру с контрольными суммами файлов инсталляционного комплекта; – копию сертификата ФСТЭК. Допустимо предоставление на бумажном носителе формуляра с требованиями по эксплуатации, приложения с контрольными суммами файлов инсталляционного комплекта, копии сертификата ФСТЭК.	Да

## 7.2 ТРЕБОВАНИЯ К ВНЕДРЕНИЮ ПАЗИ

### 7.2.1 ТРЕБОВАНИЯ К ОКАЗАНИЮ УСЛУГ

Исполнитель должен оказать услуги по внедрению программного обеспечения системы анализа защищенности информации в соответствии с требованиями пояснительной записки на создание КСОИБ ЗОКИИ Общества (02409271.26.20.40.140.139.П2) (Приложение № 3 к Договору) и данного технического задания.

Услуги по внедрению ПАЗИ проводятся в соответствии с п. 3.2.5 и п. 3.3.5 «02409271.26.20.40.140.139.П2» Пояснительной записки на создание КСОИБ (Приложение № 3 к Договору) и разработанной Исполнителем документацией.

Перед началом оказания услуг по внедрению ПАЗИ Исполнитель должен проработать детальную конфигурацию ПАЗИ, перечень настроек, политик, актуализировать логические схемы взаимодействия, разработать программу и методику приемочных испытаний и согласовать проектные решения с Заказчиком.

В рамках внедрения ПАЗИ Исполнитель должен оказать следующие услуги:

1. Исполнитель должен осуществить поставку лицензий на ПО ПАЗИ в соответствии с техническими характеристиками и комплектностью, приведенными в Таблице № 1.
2. Провести анализ имеющейся проектной документации на создание ПАЗИ (Приложение № 3 к Договору) и существующих бизнес-процессов Заказчика.
3. Проработать детальную конфигурацию системы, перечень настроек, политик, логические схемы взаимодействия, разработать программу и методику приемочных испытаний и согласовать с Заказчиком.
4. Разработать и согласовать с Заказчиком эксплуатационную, рабочую и исполнительную документацию для ПАЗИ КСОИБ ЗОКИИ Общества.
5. Разработать требования по подготовке инфраструктуры Заказчика для внедрения ПО ПАЗИ.
6. Выполнить установку и настройку операционной системы для сервера управления.
7. Выполнить установку и настройку ПО ПАЗИ на подготовленный виртуальный сервер.
8. Произвести настройку ПАЗИ на получение точного времени от находящегося в сегменте «Телескоп+» сервера времени.
9. Настроить интеграцию ПАЗИ со смежными системами.
10. Настройка аудита и категоризация активов.
11. Настройка правил и политик управления выявленными уязвимостями.
12. Разработать отчёты по уязвимостям, узлам и компонентам. Настроить шаблоны отчётов.
13. Подготовить комплект документации техно-рабочего проекта.
14. Провести предварительные испытания.
15. Осуществить опытную эксплуатацию.
16. Провести приемочные испытания.

Услуги должны выполняться специалистами Исполнителя в соответствии с нормами и требованиями законодательства Российской Федерации в области охраны труда, противопожарной безопасности, безопасности производства работ, корпоративными стандартами и требованиями нормативных документов Общества, регламентирующих вопросы информационной безопасности.

Услуги должны выполняться в рабочее время по графику работы Заказчика. Выполнение работ/услуг в нерабочие часы допускается по предварительному согласованию с Заказчиком.

Услуги должны выполняться без прерывания доступности существующих сервисов Заказчика. В случае если для выполнения работ требуется прерывание какого-либо сервиса Заказчика, время выполнение таких работ должно согласовываться с Заказчиком. Предоставление технологических окон для выполнения работ/услуг с прерыванием сервиса обеспечивается Заказчиком.

Выполнение работ/услуг не должно привести к ухудшению функционирования информационной инфраструктуры и технологических процессов Заказчика.

Специалисты Исполнителя должны обладать необходимыми для выполнения работ/услуг компетенциями и опытом, иметь необходимые сертификаты на проведение



работ/услуг, если это требуется в соответствии с законодательством РФ и/или положениями данного технического задания.

ПАЗИ должна быть рассчитана на эксплуатацию в составе КСОИБ ЗОКИИ Заказчика. Техническая и физическая защита аппаратных компонентов системы, носителей данных, бесперебойное энергоснабжение, резервирование ресурсов, текущее обслуживание реализуется техническими и организационными средствами, предусмотренными в ИТ инфраструктуре Заказчика.

Во время испытаний согласно ПиМИ должны быть проведены работы/услуги по проверке работоспособности ПО ПАЗИ для существующих на момент внедрения ПО ПАЗИ подсистем инфраструктуры ИТ, АРМ и серверов КСОИБ ЗОКИИ, АРМ и серверов ЗОКИИ. Ориентировочное количество подсистем ИТ и КСОИБ – не менее 10. Ориентировочное количество АРМ и серверов КСОИБ ЗОКИИ – не менее 10. Ориентировочное количество типовых АРМ и серверов ЗОКИИ – не менее 10. Для типовых АРМ и серверов допускается проводить проверки для не более двух АРМ или серверов одного типа. Количество подсистем, АРМ и серверов КСОИБ ЗОКИИ и АРМ и серверов ЗОКИИ на момент проведения испытаний согласно ПиМИ должно быть уточнено. Результаты проверок должны быть отражены в протоколах испытаний.

В процессе подготовки к выполнению работ/услуг Исполнитель должен разработать и согласовать с Заказчиком План внедрения, включающий детальное описание хода оказания услуг.

По необходимости должны организовываться встречи Заказчика с представителями Исполнителя посредством аудио- или видеоконференций для определения состояния ИТ-проекта и решения оперативных вопросов.

Исполнитель должен документировать все согласованные в результате рабочих совещаний с Заказчиком изменения требований к настраиваемому функционалу ПО ПАЗИ.

Выполнение работ/услуг по внедрению ПАЗИ может производиться дистанционно.

Все работы/услуги в рамках данного технического задания должны проводиться при участии специалистов Заказчика.

## **7.2.2 ТРЕБОВАНИЯ К ПАЗИ И ЕЁ ФУНКЦИЯМ**

Архитектура ПАЗИ должна быть централизованной и позволять вести централизованный контроль всех устройств из единой точки.

ПАЗИ предназначена для анализа защищенности ИТ-инфраструктуры, управления ИТ-активами, выявления, приоритизации и контроля устранения уязвимостей, а также контроля соответствия стандартам и политики безопасности Заказчика.

ПАЗИ должна обеспечивать высокую производительность для решения возложенных задач, осуществлять одновременную работу нескольких пользователей, а также обладать высокой надежностью и отказоустойчивостью. ПАЗИ должна предусматривать возможность масштабирования по производительности и объему обрабатываемой информации без модификации ее программного обеспечения путем модернизации используемого комплекса



технических средств. Возможности масштабирования должны обеспечиваться средствами используемого базового программного обеспечения.

ПАЗИ должна обеспечивать возможность исторического хранения данных с глубиной не менее 3 лет.

ПАЗИ должна обеспечивать возможность создания резервных образов компонентов и их последующего развертывания в инфраструктуре Заказчика.

ПАЗИ должна обеспечивать возможность планового отключения для выполнения профилактических мероприятий, изменений или наращивания аппаратного обеспечения, установки обновлений на программное обеспечение.

Работа ПАЗИ не должна препятствовать штатному функционированию компонентов ИТ-инфраструктуры Заказчика, в том числе смежных ИС.

Общие требования к архитектуре и функциональности могут быть уточнены на этапе технического проектирования.

### **7.2.3 ТРЕБОВАНИЯ К ПОЛЬЗОВАТЕЛЬСКОМУ ИНТЕРФЕЙСУ**

Взаимодействие пользователей и администраторов ПАЗИ с прикладным программным обеспечением, входящим в состав ПАЗИ, должно осуществляться посредством визуального графического веб-интерфейса через браузеры:

- Google Chrome версии 126 или выше;
- Mozilla Firefox версии 127 или выше;
- Microsoft Chromium Edge 126 или выше;
- Яндекс.Браузер 24.6.1 или выше.

Взаимодействие пользователей и администраторов ПАЗИ с прикладным программным обеспечением, входящим в состав системы должно осуществляться посредством визуального графического интерфейса (GUI). Интерфейс системы должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Средства редактирования информации должны удовлетворять принятым соглашениям в части использования функциональных клавиш, режимов работы, поиска, использования оконной системы. Ввод-вывод данных системы, приём управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям системы.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т.п. элементов. Клавиатурный режим ввода должен использоваться главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на русском языке.



ПАЗИ должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях ПАЗИ должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Экранные формы должны проектироваться с учётом требований унификации:

- Все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации.
- Для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы. Термины, используемые для обозначения типовых операций (добавление информационной сущности, редактирование поля данных), а также последовательности действий пользователя при их выполнении, должны быть унифицированы.
- Внешнее поведение сходных элементов интерфейса (реакция на наведение указателя «мыши», переключение фокуса, нажатие кнопки) должны реализовываться одинаково для однотипных элементов. ПАЗИ должна соответствовать требованиям эргономики и профессиональной медицины при условии комплектования высококачественным оборудованием (ПЭВМ, монитор и прочее оборудование), имеющим необходимые сертификаты соответствия и безопасности Росстандарта.

#### 7.2.4 РЕШЕНИЯ ПО ВЗАИМОСВЯЗЯМ СИСТЕМЫ

Для взаимодействия ПАЗИ с АРМ/Серверами инфраструктуры ЗОКИИ должны использоваться технические учетные записи, включаемые на период проведения сканирования.

Перечень сетевых взаимодействий подсистемы контроля привилегированного доступа представлен в таблице №2.

Таблица №2

##### Перечень сетевых взаимодействий ПАЗИ

№	Компонент-источник	Система назначения	Протокол:Порт	Примечание
1.	АРМ управления СЗИ (ВМ)	Сканер уязвимостей	HTTPS:443	Управление
2.	Сканер уязвимостей	АРМ/Сервер Телескоп +	WMI SSH:22	Windows/Linux
3.	Сканер уязвимостей	Сетевое оборудование	SSH:22	АСО

Сетевые взаимодействия ПАЗИ уточняются при проектировании.

### 7.2.5 ТРЕБОВАНИЯ К НАДЕЖНОСТИ

ПАЗИ должна сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

- при сбоях в системе электроснабжения аппаратной части, приводящих к перезагрузке ОС, восстановление работы информационной системы должно происходить в автоматическом режиме после перезапуска ОС и запуска прикладного программного обеспечения;
- при ошибках в работе аппаратных средств восстановление производится силами инженеров поддержки Заказчика и/или в рамках заключенных контрактов на поддержку оборудования;

Для защиты аппаратуры от скачков напряжения и коммутационных помех должны применяться источники бесперебойного питания.

Информация, хранящаяся в системе, должна быть защищена от удаления или искажения при авариях или сбоях, в том числе:

- при разрыве связи между рабочим местом пользователя системы и сервером;
- при отказах программного обеспечения сервера;
- при отказах технических средств системы в связи с отсутствием электропитания.

Аппаратный сбой, возникший в любой момент времени работы любого клиентского места, должен приводить к отмене незавершенного действия (транзакции). При этом не должна нарушаться целостность базы данных ПАЗИ.

Программное обеспечение ПАЗИ должно восстанавливать свое функционирование при корректном перезапуске аппаратных средств. Должна быть предусмотрена возможность организации автоматического и (или) ручного резервного копирования данных системы средствами системного и базового программного обеспечения (ОС, СУБД, прикладные системы резервного копирования), входящего в состав программно-технического комплекса.

Для сохранения информации, размещаемой в системе, в случае нарушения работы сервера должен быть реализован механизм резервного копирования баз данных. Резервное копирование должно предусматриваться в автоматическом режиме, и выполняться на сервер хранения резервных копий Заказчика.

Сохранность информации в ПАЗИ должна обеспечиваться при следующих аварийных ситуациях:

- нарушения электропитания;
- нарушение или выход из строя канала связи;
- полный или частичный отказ серверов ПАЗИ, включая сбои и отказы накопителей на жестких дисках;
- сбой общесистемного программного обеспечения;
- ошибки в работе обслуживающего персонала;
- выход из строя сервера администрирования;
- выход из строя элемента сетевой инфраструктуры ПАЗИ.



## 7.2.6 ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Максимальный уровень конфиденциальности информации, обрабатываемой в ПАЗИ – для внутреннего пользования.

ПАЗИ должна удовлетворять всем требованиям регламентирующих документов Общества по информационной безопасности для возможности обработки информации максимального уровня конфиденциальности - для внутреннего пользования.

Для защиты ПАЗИ при передаче информации по каналам связи из одной ИС в другую необходимо предусмотреть использование межсетевых экранов.

Средства вычислительной техники ПАЗИ, подключаемые к корпоративной сети Общества, должны размещаться в локальных вычислительных сетях, в которых выполнены требования Общества к защите локальных вычислительных сетей. В случае использования каналов связи, выходящих за пределы контролируемой зоны, необходимо применять защищенные каналы связи, защищенные волоконно-оптические линии связи либо средства криптографической защиты информации.

Должна быть обеспечена своевременная установка обновлений информационной безопасности на прикладное и системное программное обеспечение компонентов ПАЗИ.

Метод аутентификации и авторизации пользователей ПАЗИ определяется Исполнителем на этапе технического проектирования и согласуется со структурными подразделениями ИТ и ИБ Заказчика.

Доступ к ПАЗИ привилегированных пользователей должен быть организован с использованием Подсистемы контроля привилегированного доступа.

В ПАЗИ должна быть реализована ролевая модель разграничения доступа. Различным группам пользователей должны назначаться различные права доступа, в рамках их должностных обязанностей, с соблюдением принципов «минимально необходимых привилегий» (least privilege) и «минимально необходимых знаний» (need to know).

Реализованные в ПАЗИ ограничения на использование средств аутентификации (пароли, PIN-коды и т.п.), должны обеспечивать выполнение требований к длине, сложности, сроку действия, установленных в Обществе.

В ПАЗИ должны выполняться требования к журналированию событий информационной безопасности. Срок хранения информации о событиях ИБ ПАЗИ в оперативном доступе должен составлять 1 год. В архивном доступе – 3 года с даты обнаружения события ИБ. Срок хранения информации уточняется при проектировании.

Для взаимодействия с ПАЗИ должны использоваться защищенные протоколы с шифрованием (SSL, SFTP и т.п.).

Перед передачей ПАЗИ в опытно-промышленную и промышленную эксплуатацию должна быть проведена оценка соответствия ПАЗИ требованиям информационной безопасности путем проведения соответствующих испытаний согласно ПиМИ, направленных

на проверку выполнения указанных в проектной документации и данном техническом задании мер безопасности.

Требования информационной безопасности могут быть уточнены на этапе технического проектирования.

### 7.2.7 ТРЕБОВАНИЯ К ИНФОРМАЦИОННОМУ ОБЕСПЕЧЕНИЮ

Состав, структура и способы организации данных в ИС должны быть определены на этапе технического проектирования.

Средства используемых операционных систем должны обеспечивать документирование и протоколирование обрабатываемой в системе информации.

Доступ к данным должен быть предоставлен только авторизованным пользователям с учетом их служебных полномочий на основе ролевой модели, а также с учетом категории запрашиваемой информации.

Технические средства, обеспечивающие хранение информации, должны использовать современные технологии, позволяющие обеспечить повышенную надежность хранения данных и оперативную замену оборудования.

Для сохранения информации, размещаемой в системе, в случае нарушения работы ПАЗИ должен быть реализован механизм резервного копирования. Резервное копирование должно предусматриваться в автоматическом и ручном режимах.

### 7.2.8 ТРЕБОВАНИЯ К ДОСТУПНОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ

Таблица 13

#### Требования к доступности и производительности

<b>РЕЖИМ РАБОТЫ СИСТЕМЫ</b>	Предполагаемый режим работы системы 24x7
<b>МАКСИМАЛЬНОЕ ВРЕМЯ ВОССТАНОВЛЕНИЯ ПОСЛЕ СБОЯ И МАКСИМАЛЬНОЕ ОКНО ПОТЕРИ ДАННЫХ</b>	MTD (Допустимое время простоя системы): 88 часов в год. Показатель доступности Системы: 98,9 % RTO – период времени, установленный для возобновления функционирования Системы после инцидента с учетом возможности предоставления доступа пользователям – 24 часа без учета праздничных и выходных дней. Максимальное окно потери данных в результате инцидента (RPO) – 24 часа без учета праздничных и выходных дней.
<b>НАГРУЗКА</b>	Максимальное количество сканируемых и контролируемых активов - не менее 250.
<b>ТРЕБОВАНИЯ К РЕЗЕРВНОМУ КОПИРОВАНИЮ И ВОССТАНОВЛЕНИЮ</b>	Должны быть предусмотрены средства резервного копирования и восстановления данных и конфигураций. Резервированию подлежат следующие типы данных: - журналы с внутренними событиями ОС и СУБД; - параметры функционирования модулей подсистем ПАЗИ. Срок хранения информации о событиях ИБ ПАЗИ в оперативном доступе должен составлять 1 год. В архивном доступе – 3 года с даты обнаружения события ИБ.



## **7.2.9 ТРЕБОВАНИЯ К ОТЧЕТНОСТИ**

ПАЗИ должна предоставлять:

- Возможность графического, текстового и табличного отображения информации в отчетах;
- Возможность автоматической отправки администраторам информационной безопасности отчетов по расписанию;
- Возможность экспорта отчетов.

## **7.3 ПОДГОТОВКА КОМПЛЕКТА ДОКУМЕНТАЦИИ**

Проектная документация на внедрение ПАЗИ должна отражать результаты проектирования и соответствовать требованиям, указанным в проектной документации на создание инфраструктуры для ПО «Телескоп+» в части, касающейся внедрения ПАЗИ.

Заказчик передает Исполнителю, ранее разработанную ПАО «Ростелеком» по договору от 15.02.2023 года № 133 проектную документацию на создание инфраструктуры для ПО «Телескоп+».

Состав передаваемой ранее разработанной проектной документации (Приложение № 3 к Договору):

- 02409271.26.20.40.140. 138.ПЗ Пояснительная записка к техническому проекту;
- 02409271.26.20.40.140. 139.П2 Пояснительная записка на создание КСОИБ;
- 02409271.26.20.40.140. 138.ПМ1 Программа и методика предварительных испытаний;
- 02409271.26.20.40.140.138.ОЭ Опытная эксплуатация;
- 02409271.26.20.40.140. 138.ПМ2 Программа и методика приемочных испытаний;
- 02409271.26.20.40.140.138.ИЗ Руководство администратора;
- 02409271.26.20.40.140. 138.П9 Описание комплекса технических средств.

Заказчик осуществляет передачу Исполнителю в электронной форме проектной документации в течение 3 (трех) рабочих дней с момента подписания Договора. Передача проектной документации осуществляется по описи по защищенным каналам связи или на электронном носителе.

Исполнитель должен выполнить актуализацию технического проекта на создание комплексной системы по обеспечению информационной безопасности в части ПАЗИ (в том числе на основе информации из Пояснительной записки к техническому проекту инфраструктуры для «Телескоп+»):

- спецификация оборудования и программного обеспечения;
- схема структурная;
- пояснительная записка к техно-рабочему проекту;

Исполнитель должен разработать рабочую документацию на создание комплексной системы по обеспечению информационной безопасности в части ПАЗИ (в том числе на основе информации из Пояснительной записки к техническому проекту инфраструктуры для «Телескоп+»):

- программа и методика испытаний (предварительных, приемочных);
- программа опытной эксплуатации;

Программа и методика испытаний должна предусматривать мероприятия по проверке работоспособности ПО ПАЗИ для существующих на момент внедрения ПАЗИ подсистем инфраструктуры ИТ, подсистем, АРМ и серверов КСОИБ ЗОКИИ, АРМ и серверов ЗОКИИ согласно п. 7.3.1 данного технического задания.

Актуализировать и разработать эксплуатационную документацию комплексной системы по обеспечению информационной безопасности в части ПАЗИ (в том числе на основе информации из Пояснительной записки к техническому проекту инфраструктуры для «Телескоп+»):

- руководство администратора;
- руководство пользователя.

По окончании работ/услуг Исполнитель должен разработать и передать Заказчику исполнительную документацию, содержащую:

- перечень созданных учетных записей и паролей ко всему поставленному и настроенному, системного и прикладному программному обеспечению;
- технический паспорт ПАЗИ, содержащий: сведения о компонентах подсистемы, IP адреса, имя сервера, перечень ПО и их версий, описание настроек программного обеспечения;
- инструкцию администратора, содержащую информацию о предварительной настройке АРМ и серверов для установки и обеспечению функционирования ПО ПАЗИ.

Документация должна быть передана в виде подлежащих текстовому редактированию файлов в формате офисных приложений Microsoft Word в электронном виде, а также в твердой копии в 2 (двух) экземплярах. Вся передаваемая Исполнителем документация должна быть составлена на русском языке.

Комплект документов следует передавать с соблюдением требований сохранения конфиденциальности информации.

Состав передаваемой Заказчику документации ПАЗИ:

- Спецификация используемого в ПАЗИ оборудования и программного обеспечения;
- Схема структурная;
- Пояснительная записка на создание ПАЗИ;
- Технический паспорт
- Программа и методика предварительных испытаний;
- Программа опытной эксплуатации;
- Программа и методика приемочных испытаний;



- Руководство администратора;
- Руководство пользователя.

## **8 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ УСЛУГ**

Контроль соответствия, разработанного в рамках данного проекта функционала ПАЗИ требованиям настоящего технического задания, планируется выполнять посредством проведения приемо-сдаточных испытаний, проводимых в несколько этапов, каждый из которых необходим для минимизации количества возможных ошибок перед началом промышленной эксплуатации.

Для ПАЗИ устанавливаются следующие виды испытаний:

- Предварительные испытания;
- Опытная эксплуатация;
- Приемочные испытания.

Испытания ПАЗИ проводятся в соответствии с разработанной Исполнителем и согласованной Заказчиком Программой и методикой испытаний (далее – ПиМИ) для ограниченного круга пользователей (пилотной группы) и на ограниченном объеме исходных данных и включают проверку:

- Полноты и качества реализации функций при штатных, предельных, критических значениях параметров объекта автоматизации и в других условиях функционирования ИС.
- Средств и методов восстановления работоспособности после отказов.
- Комплектности и качества эксплуатационной документации.

По результатам проведения каждого из этапов испытаний согласно ПиМИ составляется Протокол и Акт проведения приемо-сдаточных испытаний. При успешном прохождении всех этапов испытаний оформляется акт о готовности ИС к вводу в промышленную эксплуатацию.

Формы Актов и Протоколов проведения приемо-сдаточных испытаний разрабатываются Исполнителем и согласуются Заказчиком на этапе разработки Программы и методикой испытаний.

В случае выявления замечаний и невозможности допуска ПАЗИ к следующему этапу испытаний, Исполнитель в согласованный с Заказчиком срок устраняет зафиксированные в Протоколе приемо-сдаточных испытаний замечания. После устранения Исполнителем выявленных замечаний назначаются повторные приемо-сдаточные испытания.

## **9 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ УСЛУГ ПО ПОДГОТОВКЕ СИСТЕМЫ К ВВОДУ В ЭКСПЛУАТАЦИЮ**

Приемка ПАЗИ должна осуществляться путем проведения приемо-сдаточных испытаний, в соответствии с требованиями ГОСТ Р 59792-2021 «Информационная технология. Виды испытаний автоматизированных систем»:

1. Предварительные испытания:

- 1.1. предварительные испытания проводятся в соответствии с утвержденной Программой и методикой испытаний в присутствии представителей Заказчика для определения работоспособности и решения вопроса о возможности приемки ПАЗИ в опытную эксплуатацию;
- 1.2. по результатам предварительных испытаний формируется Протокол, который должен содержать заключение о возможности (невозможности) приемки ПАЗИ в опытную эксплуатацию, а также перечень необходимых доработок и рекомендуемые сроки их выполнения;
- 1.3. предварительные испытания завершаются оформлением акта приемки ПАЗИ в опытную эксплуатацию.

2. Опытная эксплуатация:

- 2.1. опытная эксплуатация ПАЗИ проводится с целью определения характеристик ПАЗИ и готовности персонала Заказчика к работе в реальных условиях функционирования ПАЗИ, а также определения фактической эффективности ПАЗИ и, при необходимости, корректировки документации;
- 2.2. по результатам опытной эксплуатации ПАЗИ принимается решение о возможности (невозможности) предъявления ПАЗИ на приемочные испытания.
- 2.3. опытная эксплуатация завершается оформлением акта о завершении опытной эксплуатации.

3. Приемочные испытания:

- 3.1. приемочные испытания ПАЗИ проводятся для определения соответствия ПАЗИ требованиям Технического задания, оценки качества опытной эксплуатации и решения вопроса о возможности ввода ПАЗИ в промышленную эксплуатацию;
- 3.2. приемочные испытания ПАЗИ проводятся Исполнителем в присутствии представителей Заказчика путем выполнения комплексных тестов согласно ПиМИ;
- 3.3. по результатам приемочных испытаний формируется Протокол, который должен содержать обобщенные результаты испытаний и выводы о результатах испытаний и соответствии ПАЗИ требованиям настоящего ТЗ, и акт о готовности ПАЗИ к вводу в опытно-промышленную эксплуатацию.

**Заказчик:**

Заместитель генерального директора по  
техническим вопросам и  
информационным технологиям



Р.Л. Шуман

М.П.

**Исполнитель:**

Заместитель директора филиала –  
директор по работе с корпоративным и  
государственным сегментами Самарского  
филиала ПАО «Ростелеком»



А.Н. Толочная

М.П.



# Спецификация

№ п/п	Наименование	Наименование в терминах Правообладателя	Артикул	Количество	Цена за единицу, руб. без НДС	Стоимость, руб. без НДС	Цена за единицу, руб. с НДС	Ставка НДС, %	Стоимость, руб. с НДС	Номер реестровой записи из единого реестра российских программ для электронных вычислительных машин и баз данных или реестра евразийского программного обеспечения Наименование правообладателя	Код ОКПД2
1	Неисключительные права использования программного обеспечения системы анализа защищенности информации	PT-MPSIEM-VM- HCC-AIO-250 Программное обеспечение MaxPatrol Security Information and Event Management. Конфигурация MaxPatrol VM HCC All-In-One для выявления уязвимостей и проверки соответствия стандартам не более 250 активов, обновления в течение 1 (одного) года	PT- MPSIEM- VM-HCC- AIO-250	1 шт.	3 392 400,00	3 392 400,00	3 392 400,00	НДС не облагает ся	3 392 400,00	№ 10583 АО "ПОЗИТИВ ТЕХНОЛОДЖИЗ"	58.29.12. 000
2	Услуги по внедрению программного обеспечения системы анализа защищенности информации		-	1 условная единица	5 892 309,28	5 892 309,28	7 070 771,14	20	7 070 771,14	-	-
	<b>ИТОГО:</b>		X	X	X	<b>9 284 709,28</b>	X	X	<b>10 463 171,14</b>	X	X

1. Итого стоимость по Спецификации составляет: 10 463 171 (Десять миллионов сорок шесть тысяч сто семьдесят один) рубль 14 копеек, в том числе НДС в сумме 1 178 461 (Один миллион сто семьдесят восемь тысяч сорок шесть рублей 86 копеек, в том числе:
  - Стоимость Лицензий составляет: 3 392 400 (Три миллиона триста девяносто две тысячи четыреста) рублей 00 копеек НДС не облагается на основании пп. 26 п. 2 ст. 149 НК РФ;
  - Стоимость Услуг составляет 7 070 771 (Семь миллионов семьдесят тысяч семьсот семьдесят один) рубль 14 копеек, в том числе НДС в сумме 1 178 461 (Один миллион сто семьдесят восемь тысяч сорок шесть рублей 86 копеек.
2. Конечный пользователь: ПАО «Самараэнерго»
3. Порядок предоставления Лицензий:
  - Передаются в электронном виде;
  - Передаются на электронную почту Заказчика: [info@samaraenergy.ru](mailto:info@samaraenergy.ru)
4. Условия предоставления Лицензий:
  - лицензии предоставляются в соответствии с общепринятым в мировой практике обычаем делового оборота – принципом «AS IS» («таким, каков он есть»).
5. Место передачи Лицензий и оказания Услуг:
  - по адресу места нахождения Заказчика: 443079, Российская Федерация, город Самара, проезд Георгия Митирева, дом 9
6. Место предоставления документов:
  - по адресу места нахождения Заказчика: 443079, Российская Федерация, город Самара, проезд Георгия Митирева, дом 9

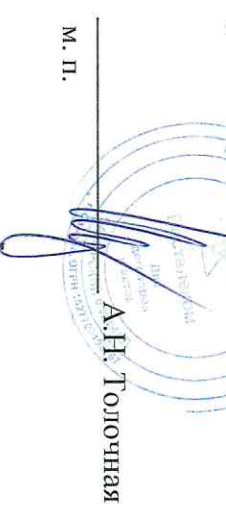
### Заказчик

Заместитель генерального директора  
по техническим вопросам и  
информационным технологиям

  
Р.Л. Шуман  
М. П.

### Исполнитель

Заместитель директора филиала – директор по работе с  
корпоративными и  
государственными сегментами Самарского  
филиала ПАО «Ростелеком»

  
А.Н. Толочная  
М. П.



**Порядок оформления запроса физического доступа на территорию Заказчика.**

Запрос (Официальное письмо) предоставления физического доступа на территорию объектов ПАО «Самараэнерго» оформляется на официальном бланке организации в произвольной форме, но со строгим соблюдением следующих требований:

1. Отсылка на действующий договор, или иной правоустанавливающий документ, на основании которого запрашивается доступ:
  - 1.1. Номер и дата договора;
  - 1.2. Предмет договора;
2. ФИО сотрудников, лица, для которых запрашивается физический доступ, но не более 5 (пяти) человек по одному договору:
  - 2.1. Фамилия Имя Отчество;
  - 2.2. Дата рождения;
3. Паспортные данные каждого из лиц, для которых запрашивается физический доступ:
  - 3.1. Номер и серия паспорта;
  - 3.2. Дата выдачи паспорта;
  - 3.3. Номер подразделения кем выдан паспорт;
4. Предельно конкретное описание цели доступа, с подробным содержанием функциональных задач каждого из сотрудников, для которых запрашивается доступ;
5. Обязательно указать старшего группы сотрудников, для решения с ним вопросов по взаимодействию с работниками заказчика по соблюдению правил внутреннего распорядка ПАО «Самараэнерго»;
6. Указание продолжительности доступа:
  - 6.1. На весь срок действия договора;
  - 6.2. Определенной даты с указанием временного промежутка в течении рабочей недели (если услуги несут разовый характер);
  - 6.3. Выходные и праздничные дни, исключительно при необходимости произвести тестирование и настройку сервисов, в нерабочее время на оборудовании ПАО «Самараэнерго» с высокой вероятностью критической нагрузки на оборудование информационной инфраструктуры. Оформляется в исключительных случаях, предварительно согласовав с начальником управления по информационным технологиям не менее чем за 14 (Четырнадцать) календарных дней;
7. Спецификация вносимого и/или выносимого оборудования:
  - 7.1. Марка, модель, серийный и/или иной идентификационный номер;
  - 7.2. Назначение изделия (детальное описание в каких целях будет использоваться данное оборудование);
8. Письмо на доступ должно быть: подписано надлежащим уполномоченным лицом, если лицо действует по доверенности, то с приложением копии такой доверенности, скреплено печатью и направлено на имя Заместителя генерального директора по техническим вопросам и информационным технологиям ПАО «Самараэнерго» на электронный адрес: [info@samaraenergo.ru](mailto:info@samaraenergo.ru) или [info2@samaraenergo.ru](mailto:info2@samaraenergo.ru) в виде цветных сканированных изображений с разрешением не менее 300DPI или почтой или курьером в виде твердой копии в цвете по адресу: 443079, город Самара, область Самарская, проезд Георгия Митирева, дом 9.

**Заказчик:**  
Заместитель генерального директора по техническим вопросам и информационным технологиям

М.П.

Р.Л. Шуман

**Исполнитель:**  
Заместитель директора филиала – директор по работе с корпоративным и государственными сегментами Самарского филиала ПАО «Ростелеком»

М.П.

А.Н. Толочная





**Порядок оформления запроса предоставления удалённого доступа (компьютерного) к сетевой инфраструктуре ПАО «Самараэнерго».**

Запрос (Официальное письмо) предоставления удалённого доступа оформляется на официальном бланке организации в произвольной форме, с соблюдением следующих требований:

1. Указание реквизитов договора для исполнения которого запрашивается доступ:
  - 1.1. Дата и номер документа (договора, письма, иного документа);
  - 1.2. Заголовок и предмет договора;
2. ФИО (полностью) лиц, для которых запрашивается удалённый доступ, но не более 5 (Пяти) человек по одному договору:
  - 2.1. Фамилия Имя Отчество;
  - 2.2. Дата рождения;
3. Указание информационной системы к которой требуется доступ с подробным описанием уровня привилегий;
4. Предельно конкретное описание цели доступа, с подробным содержанием функциональных задач каждого представителя, для которого запрашивается доступ;
5. Указание продолжительности доступа:
  - 5.1. На весь срок действия договора (проведение длительных технических работ);
  - 5.2. Определенной даты с указанием временного промежутка в течении рабочей недели (проведение технических работ разового характера);
6. Адрес служебной электронной почты каждого представителя, для которого запрашивается доступ (адрес, который использует представитель, электронные почтовые сообщения с которого регулярно читает);
7. Номер мобильного телефона представителя, для которого запрашивается доступ, который реально используется таким лицом, постоянно ему доступный;
8. Запрос должен быть подписан надлежащим уполномоченным лицом, если лицо действует по доверенности, то с приложением копии такой доверенности, и печатью (при наличии) и адресовано заместителю генерального директора по техническим вопросам и информационным технологиям ПАО «Самараэнерго» с официального адреса электронной почты, указанной в договоре на оказание услуг, на электронный адрес: [info@samaraenergo.ru](mailto:info@samaraenergo.ru) в виде цветных сканированных изображений с разрешением не менее 200DPI или почтой или курьером оригинала документа по адресу: 443079, город Самара, область Самарская проезд Георгия Митирева, дом 9.

**Заказчик:**

Заместитель генерального директора по техническим вопросам и информационным технологиям

М.П.

Р.Л. Шуман

**Исполнитель:**

Заместитель директора филиала – директор по работе с корпоративным и государственным сегментами Самарского филиала ПАО «Ростелеком»

М.П.

А.Н. Толочная





**Соглашение о конфиденциальности**

г. Самара

«14» 10 2025г.

Публичное акционерное общество энергетики и электрификации «Самараэнерго» (ПАО «Самараэнерго»), именуемое в дальнейшем (далее- Заказчик), в лице Заместителя генерального директора по техническим вопросам и информационным технологиям Шумана Родиона Львовича, действующего на основании доверенности № 30 от 29.12.2024 года, с одной стороны, и Публичное акционерное общество «Ростелеком» (ПАО «Ростелеком») (далее – Исполнитель), в лице Заместителя директора филиала - директора по работе с корпоративным и государственным сегментами Самарского филиала ПАО «Ростелеком» Толочной Анастасии Николаевны, действующего на основании доверенности № 0607/29/45/24 от 19.11.2024, с другой стороны, в дальнейшем совместно именуемые «Стороны», а по отдельности «Сторона», принимая во внимание, что в связи с возможностью заключения и исполнения Сторонами Договора на передачу Заказчику на условиях простой (неисключительной) лицензии право использования программного обеспечения системы анализа защищенности информации (далее – Лицензии) и оказания услуг по внедрению программного обеспечения системы анализа защищенности информации.

Исполнитель и Заказчик, обсудив возможность передачи Сторонами друг другу определенной информации конфиденциального характера о Сторонах, коммерческой деятельности и операциях Сторон, заключили настоящее соглашение о конфиденциальности о нижеследующем:

**1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

Для целей настоящего Соглашения Стороны соглашаются использовать следующие термины и определения:

1.1. **«Конфиденциальная информация»** - любая информация (сведения, сообщения, данные) о лицах, предметах, фактах, событиях, явлениях и процессах, обозначенная Передающей Стороной в качестве Конфиденциальной информации и переданная в соответствии с порядком, указанным в настоящем Соглашении.

**«Конфиденциальная информация»** не включает в себя информацию, которая (является общедоступной, либо была доступна Получающей Стороне не на конфиденциальной основе до передачи этой информации Передающей Стороной, либо становится доступна Получающей Стороне не на конфиденциальной основе из какого-либо источника помимо Передающей Стороны, при условии, что Получающей Стороне известно, что этому источнику не запрещено раскрывать такую информацию договорным или иным юридическим обязательством перед Передающей Стороной.

1.2. **«Стороны»** - означает Заказчик и Исполнитель.

1.3. **«Передающая Сторона»** - сторона, которой может быть, как Исполнитель, так и Заказчик, передающая на условиях настоящего Соглашения Конфиденциальную информацию.

1.4. **«Получающая Сторона»** - сторона, которой может быть, как Исполнитель, так и Заказчик, получающая от Передающей Стороны на условиях настоящего Соглашения Конфиденциальную информацию

1.5. **«Представители»** - директора, работники, аудиторы и аффилированные лица Стороны, которые уполномочены передавать и/или получать Конфиденциальную информацию.

1.6. **«Третьи лица»** - иные лица, не относящиеся к Сторонам и их Представителям.

1.7. **«Разглашение Конфиденциальной информации»** – действие или бездействие Получающей Стороны, в результате которого переданная по Соглашению Конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной Третьим лицам без согласия Передающей Стороны.



1.8. «Соглашение» - означает настоящее Соглашение о конфиденциальности с учетом изменений и дополнений, которые могут быть внесены Сторонами в настоящее Соглашение.

## **2. ПРЕДМЕТ СОГЛАШЕНИЯ**

2.1. Настоящее Соглашение распространяется на Конфиденциальную информацию, передаваемую Передающей Стороной Получающей Стороне в связи с Договором, а также Конфиденциальную информацию, которая иным образом станет известной Получающей Стороне в связи с Договором (в указанном случае Передающая Сторона в письменной форме уведомляет Получающую Сторону о том, что такая информация является Конфиденциальной информацией).

2.2. Настоящим Стороны подтверждают, что в рамках исполнения Соглашения не планируется передача/получение информации, в отношении которой введен режим коммерческой тайны в соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

2.3. Передача Конфиденциальной информации осуществляется на бумажных и иных материальных носителях, содержащих отметку о конфиденциальности (грифы «Конфиденциальная информация» / «Конфиденциально» с указанием наименования и местонахождения Передающей Стороны).

2.4. Стороны соглашаются с тем, что Конфиденциальная информация может быть передана Передающей Стороной Получающей Стороне по электронной почте:

- в зашифрованном виде с использованием программного комплекса средств шифрования передаваемой информации по алгоритму ГОСТ;

- в заархивированном виде (на архив должен быть установлен пароль не менее 8 символов и содержать буквы в верхнем и нижнем регистрах, цифры и спецсимволы, пароль должен быть передан альтернативным каналом связи).

2.5. При передаче Конфиденциальной информации по электронной почте в сообщении должно быть указано, что передаваемая информация является Конфиденциальной информацией.

2.6. Передача Конфиденциальной информации должна осуществляться на основании акта приема-передачи, форма которого представлена в Приложении № 1 к настоящему Соглашению.

2.7. В случае раскрытия Конфиденциальной информации в устном виде Стороны обязуются в течение 3 (трех) рабочих дней с момента устного раскрытия оформить передачу такой Конфиденциальной информации на бумажных и иных материальных носителях или по электронной почте в соответствии с настоящим пунктом Соглашения.

2.8. Передача Конфиденциальной информации способами, не предусмотренными настоящим пунктом Соглашения, запрещается.

## **3. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

3.1. Получающая Сторона вправе предоставлять доступ к полученной по настоящему Соглашению Конфиденциальной информации только тем Представителям Получающей Стороны, доступ которых к Конфиденциальной информации необходим в связи с Договором, и только в той части, в которой это необходимо. При этом Представители Получающей Стороны, получившие доступ к такой информации, должны быть уведомлены Получающей Стороной о конфиденциальности информации и условиях ее использования. Перечень Представителей Получающей Стороны, которым будет предоставлен доступ к Конфиденциальной информации, должен быть передан Получающей Стороной Передающей Стороне до предоставления им доступа к Конфиденциальной информации.

3.2. Получающая Сторона соглашается, что Конфиденциальная информация будет использована исключительно в связи с Договором и что Получающая Сторона и ее Представители сохраняют конфиденциальность такой информации, и эта информация не будет раскрыта или передана Третьим лицам без предварительного письменного согласия Передающей Стороны.



3.3. Получающая Сторона обязуется обеспечить защиту полученной Конфиденциальной информации на уровне не меньшем, чем осуществляется защита Конфиденциальной информации Передающей Стороны.

3.4. В случае передачи Получающей Стороной на основании письменного согласия Передающей Стороны Конфиденциальной информации Третьим лицам, Получающая Сторона обязана обеспечить, чтобы Третьи лица до момента передачи им Конфиденциальной информации приняли на себя обязательства по использованию и неразглашению такой информации на условиях, предусмотренных в настоящем Соглашении. Получающая Сторона обязана до момента передачи Третьим лицам Конфиденциальной информации предоставить Передающей Стороне копию соглашения о конфиденциальности, подписанного Получающей Стороной с Третьим лицом.

3.5. В случае получения мотивированного требования от органа государственной власти или органа местного самоуправления о предоставлении Конфиденциальной информации, полученной по настоящему Соглашению, Получающая Сторона обязана:

- уведомить соответствующий орган государственной власти или орган местного самоуправления о конфиденциальности такой информации и ее обладателе;
- если это не запрещено действующим законодательством Российской Федерации, незамедлительно известить в письменной форме о таком требовании Передающую Сторону для того, чтобы Передающая Сторона имела возможность принять меры в порядке ограничения или предотвращения предоставления соответствующей Конфиденциальной информации.

3.6. Получающая Сторона имеет право на основании мотивированного требования предоставить органу государственной власти или органу местного самоуправления лишь ту часть полученной от Передающей Стороны Конфиденциальной информации, предоставление которой требуется по закону.

#### **4. ОТВЕТСТВЕННОСТЬ СТОРОН**

4.1. Получающая Сторона несет ответственность за нарушение обязательств по соблюдению условий использования и обеспечения конфиденциальности полученной Конфиденциальной информации в соответствии с законодательством Российской Федерации и условиями настоящего Соглашения и обязана возместить Передающей Стороне убытки, возникшие у Передающей Стороны вследствие ненадлежащего исполнения Получающей Стороной условий настоящего Соглашения.

4.2. Получающая Сторона несет ответственность в полном объеме за Разглашение Конфиденциальной информации ее Представителями и Третьими лицами, получившими доступ к такой информации в соответствии с условиями, определенными в пунктах 3.1. и 3.2. настоящего Соглашения.

4.3. При Разглашении Конфиденциальной информации, а также при наличии обстоятельств, способствующих Разглашению Конфиденциальной информации, Получающая Сторона обязана незамедлительно уведомить об этом Передающую Сторону в письменной форме, предоставить Передающей Стороне всю необходимую информацию о факте Разглашения или наличии угрозы Разглашения, причинах, приведших к этому, и мерах, предпринятых Получающей Стороной для предотвращения Разглашения и устранения возникших в связи с этим неблагоприятных последствий.

#### **5. РАЗРЕШЕНИЕ СПОРОВ**

5.1. Отношения, возникающие из настоящего Соглашения, регулируются правом Российской Федерации.

5.2. Все споры и разногласия по настоящему Соглашению Стороны разрешают путем переговоров.

5.3. Претензионный порядок урегулирования споров будет применяться Сторонами в случаях, предусмотренных законом. Претензия в рамках настоящего Соглашения должна быть направлена в порядке, предусмотренном п. 7.2. Соглашения. Срок рассмотрения претензии - 10 (десять) рабочих дней с момента ее доставки.

5.4. В случае если споры и разногласия не урегулированы в соответствующем порядке, определенном в п. 5.2. и п. 5.3. Соглашения, каждая из Сторон вправе обратиться с иском о разрешении спора в Арбитражный суд Самарской области.





## 6. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

6.1. Настоящее Соглашение вступает в силу с даты его подписания обеими Сторонами и действует в течение срока действия Договора, а также в течение 3 (Трех) лет по окончании его действия, если иное не будет согласовано Сторонами.

6.2. Обязательства Получающей Стороны по сохранению конфиденциальности полученной от Передающей Стороны Конфиденциальной информации, определенные в настоящем Соглашении, сохраняют силу в течение 10 (десяти) лет после истечения срока действия настоящего Соглашения.

## 7. ПРОЧИЕ УСЛОВИЯ

7.1. Получающая Сторона назначит и уведомит Передающую Сторону об уполномоченных Представителях, ответственных за контроль соблюдения обязательств по Соглашению, не позднее 3 (трех) рабочих дней со дня подписания настоящего Соглашения обеими Сторонами. Об изменении уполномоченных Представителей Получающая Сторона обязана уведомить Передающую Сторону не позднее 5 (пяти) рабочих дней до момента такого изменения.

7.2. Все уведомления и сообщения, направляемые Сторонами друг другу в соответствии с Соглашением или в связи с ним, должны быть совершены в письменной форме и должны быть переданы заказным письмом, доставлены курьером или переданы уполномоченным представителем по следующим адресам:

Исполнитель (ПАО «Ростелеком»): г. Самара, ул. Красноармейская, 17

Заказчик (ПАО «Самараэнерго»): г. Самара, проезд Георгия Митирева, д.9

В случае изменения почтового адреса Сторона обязана уведомить другую Сторону не позднее 5 (пяти) рабочих дней до момента такого изменения.

7.3. Получающая Сторона признает, что ни Передающая Сторона, а также никто из ее Представителей не дает никаких заверений или гарантий относительно полноты Конфиденциальной информации. Передающая Сторона не несет ответственности за результаты использования Конфиденциальной информации Получающей Стороной, ее Представителями или иными лицами, которым она может быть передана в соответствии с условиями настоящего Соглашения.

7.4. Передающая Сторона настоящим гарантирует, что она обладает всеми правами в отношении Конфиденциальной информации, включая право передавать такую информацию Получающей Стороне на условиях настоящего Соглашения.

7.5. Передающая Сторона вправе потребовать от Получающей Стороны вернуть ей переданные материальные носители Конфиденциальной информации, направив Получающей Стороне уведомление о возврате в письменной форме. Получающая Сторона обязана вернуть все полученные материальные носители Конфиденциальной информации и уничтожить все копии такой информации и ее воспроизведения в любой форме (включая компьютерные записи и файлы), находящиеся в распоряжении Получающей Стороны, а также в распоряжении лиц, которым такая информация была передана в соответствии с Соглашением, в срок, указанный в уведомлении, но не позднее 10 (десяти) рабочих дней после получения такого уведомления. Получающая Сторона вправе оставить Конфиденциальную информацию, необходимую для целей соблюдения требований законодательства Российской Федерации или мотивированного требования органа государственной власти или органа местного самоуправления (в течение времени, предусмотренного действующим законодательством Российской Федерации).

7.6. Передающая Сторона имеет право прекратить защиту конфиденциальности, переданной ею по настоящему Соглашению Конфиденциальной информации, о чем в обязательном порядке должна письменно проинформировать Получающую Сторону в течение 10 (десяти) рабочих дней с момента принятия решения о прекращении защиты.

7.7. Положения настоящего Соглашения имеют приоритетное значение по отношению к любым другим соглашениям Сторон по Договору и включенным в них нормам о конфиденциальности, регулирующим те же и/или аналогичные отношения между Сторонами.

7.8. 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.



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

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

7.11. Недействительность или невозможность исполнения любого положения настоящего Соглашения не влияет на действительность или возможность исполнения как любых иных положений Соглашения, так и Соглашения в целом.

7.12. Настоящее Соглашение составлено на русском языке в 2 (двух) экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

## 8. АДРЕСА И РЕКВИЗИТЫ СТОРОН

### Заказчик:

Наименование полное: Публичное  
акционерное общество энергетики и  
электрификации «Самараэнерго»  
Наименование сокращенное:  
ПАО «Самараэнерго»  
Адрес полный из ЕГРЮЛ: 443079, область  
Самарская, город Самара, проезд Георгия  
Митирева, дом 9  
Адрес почтовый для корреспонденции:  
443079, Российская Федерация, город Самара,  
проезд Георгия Митирева, дом 9  
Телефон: (8-846) 340-38-63  
ИНН 6315222985, КПП 997650001,  
ОГРН 1026300956131, ОКПО 00102504  
р/с 40702810054400031730  
в Поволжском банке  
ПАО «Сбербанк России»,  
БИК 043601607,  
к/с 30101810200000000607  
e-mail: [info@samaraenergo.ru](mailto:info@samaraenergo.ru)

Заместитель генерального директора  
по техническим вопросам и  
информационным технологиям



Р.Л. Шуман

М.П.

### Исполнитель:

Наименование полное: Публичное  
акционерное общество «Ростелеком»  
Наименование сокращенное: ПАО  
«Ростелеком»  
Юридический адрес (местонахождение):  
191167, город Санкт-Петербург, вн. тер. г.  
Муниципальный округ Смольнинское,  
Синопская набережная, дом 14, литера А  
Почтовый адрес: Российская Федерация,  
115172, г. Москва, ул. Гончарная, дом 30  
Фактический адрес: Российская Федерация,  
443010, г. Самара, ул. Красноармейская, 17  
ИНН 7707049388 КПП 784201001  
КПП по месту нахождения филиала  
631543001  
ОГРН 1027700198767  
ОКПО 17514186  
р/с 40822810338000000002  
к/с 30101810400000000225  
ПАО СБЕРБАНК  
БИК 044525225  
Тел/факс: (846) 332-10-20, (846) 340-05-10  
(факс)  
e-mail: [director@volga.rt.ru](mailto:director@volga.rt.ru)

Заместитель директора филиала - директор  
по работе с корпоративным и  
государственным сегментами Самарского  
филиала ПАО «Ростелеком»



А. Н. Толочная

М.П.

ФОРМА АКТА ПРИЕМА-ПЕРЕДАЧИ  
МАТЕРИАЛЬНЫХ НОСИТЕЛЕЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Акт приема-передачи Конфиденциальной информации

г. \_\_\_\_\_ «\_\_\_\_» \_\_\_\_\_ 20\_\_ г.

В соответствии с Соглашением о конфиденциальности № \_\_\_\_\_ от \_\_\_\_\_ 20\_\_ г.  
(наименование Передающей Стороны) передало \_\_\_\_\_ (наименование  
Получающей Стороны) нижеуказанные материальные носители конфиденциальной информации:

№ п/п	Наименование передаваемой конфиденциальной информации (наименование документа)	Вид носителя информации	Количество листов / объем информации на электронном носителе	Количество экземпляров
	Аутентификационные и идентификационные данные для удаленного доступа к ИС	Электронная почта Адресат: @ Адресант: @	Зашифрованный архив в формате *.zip., название файла, размер файла	
	Аутентификационные и идентификационные данные для локального доступа к ИС			
	Сетевой адрес (IP) и порт для подключения к информационной инфраструктуре ПАО «Самараэнерго»			
	Задействованные сетевые адреса и порты информационной инфраструктуры ПАО «Самараэнерго»			
	Перечень программного обеспечения и используемые версии ИС			
	Конфигурация и настройки ИС			
	Перечень оборудования и используемые версии			

Настоящий Акт составлен в 2 (двух) экземплярах, имеющих равную юридическую силу, по одному для каждой Стороны.

От \_\_\_\_\_ (наименование Передающей Стороны) материальные носители передал  
\_\_\_\_\_ (Должность, ФИО),  
а от \_\_\_\_\_ (наименование Получающей Стороны) материальные носители получил  
\_\_\_\_\_ (Должность, ФИО).

От имени  
**Заказчика**

\_\_\_\_\_  
(необходимо указать ФИО и  
должность подписанта)

От имени  
**Исполнителя**

\_\_\_\_\_  
(необходимо указать ФИО и  
должность подписанта)

**Форма Акта согласована**

**Заказчик:**

Заместитель генерального директора по  
техническим вопросам и  
информационным технологиям

М.П.

Р.Л. Шуман

**Исполнитель:**

Заместитель директора филиала –  
директор по работе с корпоративным и  
государственным сегментами Самарского  
филиала ПАО «Ростелеком»

М.П.

А.Н. Толочная



**ОБЯЗАТЕЛЬСТВО**  
**о неразглашении сведений конфиденциального характера**  
**и соблюдения требований по защите информации.**

Я, \_\_\_\_\_  
(Фамилия, имя, отчество)

исполняющий(ая) должностные обязанности по занимаемой должности

\_\_\_\_\_  
(должность, наименование организации)

Предупрежден(а), что на период исполнения работ в соответствии с условиями настоящего договора, мне будет предоставлен доступ к конфиденциальной информации, не содержащим сведений, составляющих государственную тайну.

Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением работ в соответствии с условиями настоящего договора.
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением работ в соответствии с условиями настоящего договора.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. В течение трех лет после прекращения права на доступ к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.
7. Соблюдать требования по защите информации в соответствии с законодательством РФ и Регламентом информационной безопасности для подрядчиков ПАО «Самараэнерго».


Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

\_\_\_\_\_  
(подпись) (расшифровка)

Дата « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_\_ г.

**Заказчик:**

Заместитель генерального директора по  
техническим вопросам и  
информационным технологиям

  
\_\_\_\_\_  
М.П. Р.Л. Шуман

**Исполнитель:**

Заместитель директора филиала –  
директор по работе с корпоративным и  
государственным сегментами Самарского  
филиала ПАО «Ростелеком»

  
\_\_\_\_\_  
М.П. А.Н. Толочная







## **Регламент информационной безопасности для подрядчиков/исполнителей**

Регламент информационной безопасности для подрядчиков/исполнителей (далее – Регламент) устанавливает требования и рекомендации, предъявляемые ПАО «Самараэнерго» (далее - Компания) к третьим лицам/поставщикам/подрядчикам (далее каждый по отдельности — Подрядчик) и необходимые для обеспечения информационной безопасности и защиты интересов Компании при использовании Подрядчиками информационных активов Компании. Настоящий Регламент применим ко всем Подрядчикам и их субподрядчикам, которые хранят, обрабатывают или имеют доступ к данным Компании. Требования настоящего Регламента в обязательном порядке включаются в договоры с Подрядчиками, которые хранят, обрабатывают или имеют доступ к данным Компании.

Любые дополнительные обязательства Подрядчика в отношении информационной безопасности по любому соглашению с Компанией являются дополнением к требованиям, изложенным в настоящем Регламенте.

В контексте настоящего Регламента термин «Информация» включает Конфиденциальную информацию, используемую в процессе осуществления коммерческой деятельности (далее — «Информация»). Конфиденциальная информация — это любая информация (сведения, сообщения, данные) о лицах, предметах, фактах, событиях, явлениях и процессах, обозначенная Компанией в качестве Конфиденциальной информации и переданная в соответствии с порядком, указанным в Соглашении о конфиденциальности.

Настоящим поясняется, что данный Регламент применим ко всей Информации, обрабатываемой Подрядчиком, в том числе, обрабатываемой при:

1. Создании;
2. Редактировании;
3. Управлении;
4. Получении доступа;
5. Получении;
6. Передаче;
7. Уничтожении;
8. Хранении или размещении на сервере в любом формате, в том числе в системах и ресурсах, находящихся в памяти средств вычислительной техники, на электронных устройствах и версии такой Информации на неэлектронных носителях.

Компания в праве запрашивать у Подрядчика сведения о применяемых Подрядчиком политик, процессов и процедур по обеспечению информационной безопасности (физической безопасности и конфиденциальности Информации).

Компания вправе приостановить доступ к Информации Компании работнику Подрядчика в случае нарушения им требований настоящего Регламента.

### **1. Общие сведения**

ПАО «Самараэнерго» в соответствии с Федеральным законом от 26.07.2017г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» является субъектом критической информационной инфраструктуры Российской Федерации. Информационные системы Компании, в соответствии с Федеральным законом от 26.07.2017г. №187-ФЗ, являются объектами критической информационной инфраструктуры Российской Федерации (далее – ОКИИ).



## 2. Законодательные нормативные акты

Обеспечение информационной безопасности ОКИИ ПАО «Самараэнерго» реализуется в соответствии с действующими законодательными правовыми актами по информационной безопасности и безопасности критической информационной инфраструктуры РФ, в том числе.:

- Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года №187-ФЗ;
- Приказ ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
- Федеральный закон «О персональных данных» от 27.07.2006 года №152-ФЗ.

Подрядчик уведомлен о том, что в соответствии со статьей 274.1 Уголовного Кодекса Российской Федерации предусмотрено наказание за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации:

Ч.1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации,

- наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до трех лет.

Ч.2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации,

- наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до трех лет.

Ч.3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанной информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам



управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации,

- наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Ч.4. Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения,

- наказываются лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Ч.5. Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия,

- наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

### **3. Правила и процедуры обеспечения информационной безопасности**

Подрядчик должен принять и соблюдать настоящий Регламент и процедуры в отношении информационной безопасности в целях создания контролируемой среды (далее - Среда), связанной с защитой конфиденциальности, целостности и доступности информации.

Подрядчик должен обеспечить подписание работниками Подрядчика, до начала работ по договору, обязательства о неразглашении сведений конфиденциального характера и соблюдения требований по защите информации в соответствии с настоящим Регламентом (далее – Обязательство), и передать оригиналы этих Обязательств Компании в течение 10 рабочих дней после подписания путем направления заказным письмом с уведомлением о вручении или передачи уполномоченному работнику Компании.

При получении от Компании информации о внесении изменений в настоящий Регламент, Подрядчик должен довести такие изменения до своих работников и субподрядчиков, выполняющих работы по договорам, заключенным с Компанией под подпись.

Доступ работникам Подрядчика для работы с Информацией Компании предоставляется только после получения Компанией указанных оригиналов Обязательств, подписанных работниками Подрядчика.

При заключении договора Подрядчик обязуется определить своего представителя в качестве единственного контактного лица по всем вопросам, связанным с информационной безопасностью. В дополнение Подрядчик должен определить представителя, ответственного за контроль соблюдения настоящего Регламента.

### **4. Правила безопасной эксплуатации ОКИИ**

При производстве работ с ОКИИ персоналу Подрядчика, запрещается:

- использовать компоненты программного и аппаратного обеспечения ОКИИ в целях, не связанных с исполнением договора;
- самостоятельно производить сборку, разборку, установку и техническое обслуживание аппаратных средств, а также допускать проведение таких работ другими лицами (кроме лиц, уполномоченных на производство таких работ);
- самостоятельно вносить какие-либо изменения в конфигурацию программно-аппаратных средств или устанавливать дополнительно любые программные и аппаратные средства, а также допускать проведение таких работ другими лицами (кроме лиц, уполномоченных на производство таких работ);



- самостоятельно создавать сетевые ресурсы или организовывать сетевые сервисы (общие сетевые диски, прокси- или веб-серверы, Wi-Fi точки доступа и т. д., кроме лиц, уполномоченных на производство таких работ);
- использовать неучтенные машинные носители информации;
- передавать свои реквизиты доступа (логин, пароль) для использования другим лицам;
- использовать персональные реквизиты доступа других лиц, а также связанные с ними права доступа и функциональные возможности;
- оставлять без личного присмотра в местах, доступных другим лицам, свои реквизиты доступа, машинные и бумажные носители, содержащие конфиденциальную информацию;
- самостоятельно изменять, без письменного или электронного обращения (заявки) Заказчика, параметры и настройки программного обеспечения ОКИИ;
- загружать в средства вычислительной техники ПАО «Самараэнерго» информацию, доступ к которой ограничен законодательством Российской Федерации и не относящуюся к исполнению договора;
- осуществлять попытки и поиск способов обхода, удаления или преодоления установленных программных и аппаратно-программных средств защиты информации;
- посещать сайты сети «Интернет» и загружать web-трафик в средства вычислительной техники ПАО «Самараэнерго» не связанными с исполнением договора;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации, которые могут привести к ознакомлению с конфиденциальной информацией посторонних лиц или к предоставлению доступа к ОКИИ посторонних лиц;
- производить перемещения технических средств ОКИИ без согласования с представителем Компании;
- выносить/вносить компоненты ОКИИ, материальные носители и прочее имущество ПАО «Самараэнерго» за пределы контролируемой зоны без согласования с представителем Компании.
- нарушать правила эксплуатации программного обеспечения и оборудования ОКИИ.

## 5. Доступ к Информации

Подрядчик должен обеспечивать, как минимум, следующие меры контроля при работе с учетными записями, когда Подрядчик обладает Информацией, принадлежащей или доверенной Компанией и находящейся за пределами Среды Компании, и (или) когда Подрядчик устанавливает удаленное подключение к Среде Компании:

1. Процесс предоставления доступа осуществлялся, исходя из рабочей потребности по выполнению должностных обязанностей (т.е. наделение минимальным объемом полномочий, исключительно исходя из необходимого уровня доступа).
2. Учетные записи для доступа к системам и приложениям должны закрепляться за каждым отдельным пользователем и быть уникальными, а не являться общими.
3. Персонал Подрядчика должен иметь уникальный идентификатор, позволяющий однозначно определить работника и организацию.
4. В ОКИИ установлены следующие требования к аутентификационной информации, при наличии технической возможности, предусмотренной производителем программных и аппаратных средств:
  - длина пароля должна быть не менее 12 символов для пользовательских учетных записей;



- длина пароля для пользовательской учетной записи не менее 12 символов;
  - длина пароля администратора учетной записи не менее 15 символов;
  - пароль не должен содержать: имя, фамилию, дату рождения, месяц, логин, название организации;
  - пароль должен содержать латинские заглавные буквы (от А до Z);
  - пароль должен содержать латинские строчные буквы (от а до z);
  - пароль должен содержать цифры (от 0 до 9);
  - пароль должен содержать отличающиеся от букв и цифр спецсимволы, например: !, \$, #, %;
  - пароль не должен содержать символы кириллицы;
  - пароль не должен содержать более 2 следующих друг за другом одинаковых символов.
  - пароль не должен содержать информацию личностного характера (например: имя, фамилию, дату рождения, месяц, логин, название организации в любых словоформах), а также основываться на словах естественного языка.
  - набор используемых символов для пароля должен состоять из букв в верхнем и нижнем регистрах, цифр и/или специальных символов (@, #, \$, &, \*, % и т.п.), если это допускается производителем;
  - смена паролей производится не реже чем через 90 дней;
  - при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.
  - в случае генерации паролей использовать псевдослучайные последовательности.
5. В ОКИИ не допускается: хранить пароли в записанном виде таким образом, чтобы они были доступны посторонним лицам; хранить пароли в открытом виде в средстве вычислительной техники; размещать пароли на ресурсах общего доступа или пересылать их по электронной почте в открытом виде; сообщать пароли посторонним лицам; применять пароли, используемые для аутентификации в ОКИИ, для доступа к иным системам; применять одинаковые пароли для различных учетных записей.
  6. В случаях создания учетной записи к ОКИИ, персонал Подрядчика должен передать идентификационные и аутентификационные данные представителю Компании способом, обеспечивающим безопасность передаваемой информации.
  7. Процесс, обеспечивающий направление уведомления Компании относительно изменений в составе персонала Подрядчика в течение 24 часов с момента такого события, если такие сотрудники имеют учетные записи или им предоставлен доступ к информационным системам Компании.

## **6. Сетевая и системная безопасность**

Подрядчик должен применять, как минимум, следующие меры сетевой и системной безопасности, когда Подрядчик обладает Информацией, принадлежащей или доверенной Компанией и находящейся за пределами Среды Компании, и (или) когда Подрядчик устанавливает удаленное подключение к Среде Компании:

1. Все программное обеспечение, установленное в средствах вычислительной техники Подрядчика должно быть обновлено до последней стабильной версии, в части установки «заплаток» или пакетов безопасности.
2. Техническое обслуживание систем Подрядчика должно осуществляться на уровне, позволяющем устанавливать последние обновления и внедрять сервисные пакеты безопасности.

Меры контроля сетевой безопасности:

1. На всех сетевых интерфейсах должны быть установлены межсетевые экраны, ограничивающие входящий и исходящий трафик, исходя из текущих потребностей.

Меры контроля системной безопасности:



1. Пользовательские устройства должны быть защищены паролем.
2. Серверы и автоматизированные рабочие места должны быть защищены от воздействия вирусов/вредоносного программного обеспечения, которое подлежит регулярному обновлению.

#### **7. Управление угрозами и уязвимостями**

Подрядчик должен проводить непрерывную оценку уязвимостей и своевременно исправлять проблемы, связанные с приложениями, операционными системами и прочими компонентами своей инфраструктуры.

#### **8. Управление активами**

Подрядчик должен обеспечивать проведение инвентаризации своих активов, включая системы/устройства и программное обеспечение, когда Подрядчик обладает Информацией, принадлежащей или доверенной Компанией и находящейся за пределами Среды Компании, и (или) когда у Подрядчика есть удаленное подключение к Среде Компании.

#### **9. Обработка Информации**

Подрядчик должен обеспечить отделение Информации от информации прочих клиентов, если у Подрядчика имеется Информация, принадлежащая или доверенная Компанией, находящаяся за пределами Среды Компании, и/или если у Подрядчика есть удаленный доступ к Среде Компании. Кроме того, Подрядчик должен быть способен составить описание прохождения Информации через его Среду.

Электронный обмен информацией между Компанией и Подрядчиком (в том числе по электронной почте, путем передачи файлов, через удаленное подключение и т. д.) должен быть защищен с помощью взаимно согласованных сервисов.

#### **10. Физическая безопасность**

Необходимо разработать и применять процедуры и физические средства контроля для защиты копий Информации на бумажных носителях и информационных систем (например, аппаратное обеспечение, программное обеспечение, документация и данные), если у Подрядчика имеется Информация, принадлежащая или доверенная Компанией, находящаяся за пределами Среды Компании, и/или если у Подрядчика есть удаленный доступ к Среде Компании.

Центры обработки данных должны находиться под физическим контролем, включая формальное управление доступом в зависимости от рабочих потребностей.

#### **11. Хранение и уничтожение записей**

Подрядчик должен хранить Информацию только в течение срока, установленного в соответствующем соглашении, кроме случаев, когда по закону требуется более длительное хранение.

При истечении срока действия договоренности Подрядчик должен вернуть и гарантированно удалить Информацию.

По запросу Компании, Подрядчик должен подтвердить, что Информация была удалена.

#### **12. Управление инцидентами информационной безопасности**

Подрядчик должен в полной мере сотрудничать с Компанией для прояснения ситуации, понимания ключевых причин и определения необходимых действий для устранения таких причин в случае фактического или предполагаемого инцидента, связанного с информационной безопасностью.

Персонал Подрядной организации обязаны незамедлительно сообщать представителю ПАО «Самараэнерго» о следующих фактах:

- нарушения целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах ОКИИ;



- утери машинных носителей информации;
- компрометации аутентификационной информации (паролей от ОКИИ или о подозрениях на их компрометацию;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ОКИИ;
- некорректного функционирования установленных на элементах ОКИИ программных и технических средств, в том числе средств защиты информации;
- попыток несанкционированного доступа (или подозрений о таких попытках) к обрабатываемой в ОКИИ информации,
- заражения вредоносным программным обеспечением или других фактах, свидетельствующих о компьютерной атаке;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ОКИИ;
- выхода из строя или неустойчивого функционирования элементов ОКИИ, а также перебоев в системе электроснабжения и связи.

### 13. Управление субподрядчиками

Настоящий Регламент информационной безопасности применяется ко всем субподрядчикам, используемым Подрядчиком, которые работают с Информацией, принадлежащей или доверенной Компанией и находящейся за пределами Среды Компании, и (или) когда Подрядчик устанавливает удаленное подключение к Среде Компании. Подрядчик несет ответственность за то, чтобы обеспечивать уведомление каждого субподрядчика о содержании Регламента информационной безопасности и его соблюдение таким субподрядчиком.

Подрядчик и субподрядчики должны заключать официальные контракты, в которых описаны необходимые меры контроля, включая меры контроля за обеспечением конфиденциальности, доступности и целостности Информации.

Подрядчику необходимо проводить первоначальные и текущие оценки в целях обеспечения соблюдения субподрядчиками Регламента информационной безопасности.

Подрядчик должен информировать Компанию и получать письменное одобрение перед использованием услуг субподрядчиков, которые либо намереваются работать с Информацией, либо будут иметь доступ к системам Подрядчика или Компании, в которых находятся Информация, а также уведомлять Компанию о том, в какой стране(-ах) будет осуществляться работа с Информацией.

#### Заказчик:


Заместитель генерального директора по техническим вопросам и информационным технологиям

  
М.П.

Р.Л. Шуман

#### Исполнитель:

Заместитель директора филиала – директор по работе с корпоративным и государственным сегментами Самарского филиала ПАО «Ростелеком»

  
М.П.

А.Н. Толочная



