

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 обнаружения вторжения (далее – Лицензии) и оказать услуги по внедрению программного обеспечения системы обнаружения вторжения (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: 21 137 366 (Двадцать один миллион сто тридцать семь тысяч триста шестьдесят шесть) рублей 64 копейки, в том числе НДС в сумме 1 957 185 (Один миллион девятьсот пятьдесят семь тысяч сто восемьдесят пять) рублей 03 копейки, в том числе:

2.1.1 Стоимость Лицензий составляет: 9 394 256 (Девять миллионов триста девяносто четыре тысячи двести пятьдесят шесть рублей) рублей 47 копеек НДС не облагается на основании пп. 26 п. 2 ст. 149 НК РФ;

2.1.2 Стоимость Услуг составляет 11 743 110 (Одиннадцать миллионов семьсот сорок три тысячи сто десять рублей) рублей 17 копеек, в том числе НДС в сумме 1 957 185 (Один миллион девятьсот пятьдесят семь тысяч сто восемьдесят пять) рублей 03 копейки.

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), детализированный акт сдачи-приемки оказанных услуг или детализированный 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 обнаружения вторжения 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 обнаружения вторжения, за исключением случаев, прямо предусмотренных правом пользования производителя/правообладателя.

## **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 обнаружения вторжения 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 ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ И  
ОКАЗАНИЕ УСЛУГ ПО ВНЕДРЕНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ  
СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ**

**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.	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
8.	Контролируемая зона	Пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.
9.	Модифицируемость	Степень простоты эффективного и рационального изменения продукта или системы без добавления дефектов и снижения качества продукта
10.	Отказоустойчивость	Способность системы, продукта или компонента работать как предназначено, несмотря на наличие дефектов программного обеспечения или аппаратных средств.
11.	Угроза	Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб или вред) для организации
12.	Уязвимость	Свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации.
13.	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.
14.	Общество	ПАО «Самараэнерго»
15.	Привилегированный пользователь	Пользователь, обладающий легитимными расширенными полномочиями в работе с корпоративными системами, включая их установку, настройку и обслуживание
16.	Специальные средства защиты информации (СЗИ)	Программные и (или) программно-аппаратные средства, внедряемые в периметре информационной системы с целью обеспечения защиты обрабатываемой информации.
17.	Структурное подразделение ИБ	Структурное подразделение Общества ответственное за обеспечение информационной безопасности объектов Общества.
18.	Структурное подразделение ИТ	Структурное подразделение Общества, ответственное за развитие информационных технологий, предоставление ИТ-сервисов, автоматизации бизнес-процессов.

№	ТЕРМИН	ОПРЕДЕЛЕНИЕ
19.	Структурное подразделение (СП)	Структурное подразделение с самостоятельными функциями, задачами и ответственностью в рамках своей компетенции, определенной Положением о структурном подразделении.

### Сокращения

№	СОКРАЩЕНИЕ	ОПРЕДЕЛЕНИЕ
1.	AD	Active Directory
2.	API	Application Programming Interface
3.	DNS	Domain name system
4.	DPI	Deep Packet Inspection
5.	FTP	File transfer protocol
6.	HTTP	Hypertext transfer protocol
7.	IAM	Identity and Access Management
8.	LDAP	Lightweight Directory Access Protocol
9.	OSI	Open Systems Interconnection
10.	OVAL	Open Vulnerability and Assessment Language, открытый язык описания и оценки уязвимостей
11.	POP3	Post Office Protocol Version 3
12.	RDP	Remote desktop protocol
13.	SCADA	Supervisory Control And Data Acquisition, программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления
14.	SIEM	Security Information and Event Management, управление событиями и информацией о безопасности
15.	SMB	Server Message Block
16.	SMTP	Simple mail transport protocol
17.	SNMP	Simple network management protocol
18.	SSO	Single Sign-on
19.	SQL	Structured query language
20.	SSH	Secure Shell
21.	TCP	Transmission Control Protocol
22.	UDP	User Datagram Protocol
23.	VNC	Virtual Network Computing
24.	IP	Internet Protocol
25.	GUI	Graphical User Interface

№	СОКРАЩЕНИЕ	ОПРЕДЕЛЕНИЕ
26.	NTP	Network Time Protocol
27.	RPO	(англ. Recovery point objective) - Максимальное окно потери данных в результате инцидента
28.	RTO	(англ. Recovery time objective) - период времени, установленный для возобновления функционирования Системы после инцидента с учетом возможности предоставления доступа пользователям.
29.	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.
30.	URL	Uniform Resource Locator
31.	VLAN	Virtual Local Area Network
32.	APM	Автоматизированное рабочее место
33.	АО	Акционерное общество
34.	АСКУЭ	Автоматизированная система коммерческого учета электроэнергии
35.	БД	База данных
36.	ВМ	Виртуальная машина
37.	ЗОКИИ	Значимый объект критической информационной инфраструктуры
38.	ИБ	Информационная безопасность
39.	ИТ	Информационная технология
40.	КИИ	Критическая информационная инфраструктура
41.	НКЦКИ	Национальный координационный центр по компьютерным инцидентам
42.	НСД	Несанкционированный доступ
43.	ОЭ	Опытная эксплуатация
44.	ПЛК	Программируемый логический контроллер
45.	ПОВ	Подсистема обнаружения вторжения
46.	ПО	Программное обеспечение
47.	ПиМИ	Программа и методика испытаний
48.	КСОИБ	Комплексная система обеспечения информационной безопасности
49.	СЗИ	Средство защиты информации
50.	СКЗИ	Средство криптографической защиты информации.
51.	СУ	Система управления
52.	СУБД	Система управления базами данных
53.	ТЗ	Техническое задание
54.	ФСТЭК	Федеральная служба по техническому и экспортному контролю

№	СОКРАЩЕНИЕ	ОПРЕДЕЛЕНИЕ
55.	ФЗ	Федеральный закон

## 2 ПРЕДМЕТ ЗАКУПКИ

Приобретение неисключительных прав использования программного обеспечения системы обнаружения вторжения и оказание услуг по внедрению программного обеспечения системы обнаружения вторжения для нужд ПАО «Самараэнерго».

## 3 ЦЕЛИ И РЕШАЕМЫЕ ЗАДАЧИ

Целью закупки является создание системы обнаружения вторжения 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 обнаружения вторжения является одной из подсистем комплексной системы обеспечения информационной безопасности ЗОКИИ Общества – подсистема обнаружения вторжений (далее - ПОВ).

Назначением внедряемой ПОВ является:

- Обнаружение сетевых угроз и аномалий трафика
- Мониторинг информационной сети и анализа трафика на уровне проприетарных протоколов
- Предупреждение инцидентов, обнаружение и ранжирование рисков на основе данных об уязвимостях, сетевых соединениях и важности активов
- Оповещения о вредоносной активности в сети и признаках эксплуатации уязвимостей
- Проверка команд, передаваемых по промышленным протоколам
- Обнаружение несанкционированных узлов и соединений
- Централизованный аудит узлов информационной сети
- Идентификация и учет устройств в информационной сети
- Анализ параметров технологических процессов

Для достижения поставленных целей Исполнителю требуется реализовать следующие задачи:

1. Осуществить передачу Заказчику программного обеспечения и сертифицированного медиа-пака программного обеспечения ПОВ, необходимых для реализации проекта и отвечающего требованиям настоящего технического задания.
2. Оказать услуги по внедрению программного обеспечения ПОВ 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 обнаружения вторжений 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 обнаружения вторжений (ПОВ).

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 ПОВ 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 ПОВ**

Оказание услуг по внедрению ПОВ 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 – 2 шт.
- ОС Astra Linux Special Edition 1.8, ФСТЭК («Воронеж», «Смоленск») – 2 шт.
- ПО ПОВ (поставляемое в рамках данного договора) – 1 шт.

Заказчик обеспечивает предоставление доступа к виртуальным серверам для развертывания ПОВ согласно Пояснительной записки (02409271.26.20.40.140.138.ПЗ) (Приложение № 3 к Договору).

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

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 наличие и работоспособность скомпонованных и настроенных должным образом межсетевых экранов для защиты ПОВ 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.

Заказчик предоставляет Исполнителю сведения об учетных записях, необходимых для настройки сетевого оборудования для передачи копии целевого трафика для анализа с использованием SPAN-портов и для настройки системы.

## **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 ПОВ 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 осуществляют его техническую поддержку.

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

Состав используемого ПО ПОВ 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 ПОВ в Обществе Исполнитель должен осуществить поставку лицензий на ПО ПОВ с техническими характеристиками, приведенными в Таблице № 1.

Таблица № 1

№ п/п	Наименование характеристики	Значение характеристики
1.	Лицензия на программное обеспечение на право пользования основной функциональностью для одного сервера - 1 шт. (KL4935RAAZS Kaspersky Industrial CyberSecurity for Networks Standard Server Russian Edition.1-Server Base License – Лицензия (Включая KL8069RMZZZ Kaspersky Certified media Pack Customized Russian) – 1 шт.	
1.1.	Срок действия лицензии	Бессрочно
1.2.	Поддержка режима пассивного анализа трафика с подключением к технологическому сегменту через SPAN-порт или TAP-устройство	Наличие
1.3.	Возможность контроль конфигураций устройств: просмотр сведений о конфигурации, ведение архива конфигураций узла, обнаружение отличий конфигурации узла от эталонной	Наличие
1.4.	Поддержка контроля конфигураций для узлов под управлением ОС семейства Windows и Linux, ПЛК и сетевых устройств (коммутаторов, маршрутизаторов и т.п.)	Наличие
1.5.	Возможность гибкой настройки мониторинга трафика: включения/отключения отдельных точек мониторинга и технологий анализа трафика	Наличие
1.6.	Возможность поддержки активного опроса сетевых узлов по протоколам (Modbus TCP, S7comm, BECKHOFF, MMS, CIP, SSH, ARP, SNMP, WMI и др.) для сбора информации об этих устройствах	Наличие
1.7.	Возможность выявления рисков системы. Обнаружение и оценка таких рисков, как неправильные настройки, уязвимости, проблемы сетевой архитектуры	Наличие
1.8.	Возможность импорта конфигураций устройств и тегов из внешних проектов (SCADA):	
1.8.1.	- Проект универсального формата - может быть получен из любых источников путем преобразования и сохранения данных в текстовых файлах с разделителями в формате CSV	Наличие
1.8.2.	- Файл конфигурации AC 800M для сервера OPC - может быть получен с помощью программного обеспечения для управления устройствами ABB AC 800M	Наличие
1.8.3.	- Проект Control Builder M - может быть получен с помощью программного обеспечения ABB Control Builder M	Наличие
1.8.4.	- Архив с конфигурацией устройств COS - может быть получен с помощью программного обеспечения для управления устройствами, поддерживающими протокол COS	Наличие
1.8.5.	- Проект DeltaV - может быть получен с помощью программного обеспечения для управления устройствами Emerson DeltaV	Наличие
1.8.6.	- Проект DirectSOFT6 - может быть получен с помощью программного обеспечения для управления устройствами DirectLOGIC	Наличие
1.8.7.	- Список тегов ABB Freelance 2016 Engineering - может быть получен с помощью программного обеспечения ABB Freelance 2016 Engineering	Наличие
1.8.8.	- Проект для устройств IEC 61850 - может быть получен с помощью программного обеспечения для управления устройствами, поддерживающими протоколы стандарта IEC 61850	Наличие
1.8.9.	- Проект RSLogix 5000 (представленный CSV- или ACD-файлом) - может быть получен с помощью программного обеспечения для управления устройствами RSLogix 5000	Наличие

№ п/п	Наименование характеристики	Значение характеристики
1.8.10.	- Проект SICAM PAS V7 (представленный TXT-файлом описания или PXD-файлом) - может быть получен с помощью программного обеспечения Siemens SICAM PAS версии 7	Наличие
1.8.11.	- Проект TIA Portal V12/V13 - может быть получен с помощью программного обеспечения Siemens TIA Portal версий 12 или 13	Наличие
1.8.12.	- Проект Schneider Electric Unity – может быть получен с помощью программного обеспечения для управления устройствами Schneider Electric серии Modicon. Проект может быть представлен ZEF- или XEF-файлами (при этом если проект представлен ZEF-файлом, то этот файл не нужно упаковывать в ZIP-архив для импорта)	Наличие
1.8.13.	- Проект WinCC (в том числе WinCC OA, WinCC flexible) - может быть получен с помощью программного обеспечения Siemens SIMATIC WinCC, WinCC OA, WinCC flexible	Наличие
1.8.14.	- Файл конфигурации YARD - может быть получен с помощью программного обеспечения для управления устройствами, поддерживающими протокол YARD	Наличие
1.8.15.	- CSV-файл экспорта SIMPLICITY - может быть получен с помощью программного обеспечения SIMPLICITY	Наличие
1.8.16.	- Файл конфигурации Valmet DNA - может быть получен с помощью программного обеспечения Valmet DNA	Наличие
1.8.17.	- XML-файл конфигурации EGD - может быть получен путем экспорта конфигурации для обмена данными по протоколу General Electric EGD	Наличие
1.8.18.	- SIG-файл проекта ControlWave - входит в состав проекта, который используют устройства Emerson серии ControlWave	Наличие
1.8.19.	- Проект Honeywell Control Builder - может быть получен с помощью программного обеспечения Honeywell Control Builder.	Наличие
1.8.20.	- Проект PcVue V10/V11 - может быть получен с помощью программного обеспечения PcVue версий 10 или 11	Наличие
1.8.21.	- CSV-файл экспорта Proficy - может быть получен с помощью программного обеспечения Proficy	Наличие
1.8.22.	- Проект с файлами экспорта Foxboro IACC - может быть получен с помощью программного обеспечения Foxboro IACC	Наличие
1.9.	Возможность анализа телеметрии технологического процесса (DPI)	Наличие
1.10.	Возможность автоматической инвентаризации узлов в наблюдаемой сети:	
1.10.1.	- Автоматическое составление списка существующих в сети узлов	Наличие
1.10.2.	- Автоматическое определение типа узлов (рабочая станция, сервер, контроллер и т.д.)	Наличие
1.10.3.	- Автоматическое определение атрибутов узлов (ОС, производитель, модель) по MAC-адресам, паттернам сетевого трафика, данным от приложений защиты конечных узлов	Наличие
1.11.	Возможность отображения сведений о сетевых сеансах	Наличие
1.12.	Поддержка визуализации сетевых взаимодействий:	
1.12.1.	- Автоматическое построение карты сетевых взаимодействий, отображающей существующие узлы и взаимодействия между ними;	Наличие
1.12.2.	- Отображение на карте сети взаимодействий, произошедших в заданный промежуток времени в прошлом;	Наличие
1.12.3.	- Автоматическое построение отображение схемы физических подключений узлов на топологической карте посредством активного опроса сетевого оборудования по протоколу SNMP	Наличие
1.13.	Возможность автоматической группировки узлов по типу, производителю, принадлежности к подсетям	Наличие
1.14.	Поддержка мониторинга сетевых подключений к технологической сети:	
1.14.1.	- Обнаружение подключения новых сетевых узлов к контролируемым сегментам технологической сети	Наличие
1.14.2.	- Обнаружение новых, ранее не наблюдавшихся сетевых коммуникаций между узлами сети	Наличие
1.14.3.	- Обнаружение внешних подключений к сегментам технологической сети (например, сессий удалённого управления)	Наличие
1.14.4.	- Обнаружение сетевых подключений к контроллерам по промышленным протоколам	Наличие

№ п/п	Наименование характеристики	Значение характеристики
1.15.	Возможность мониторинга управляющих сетевых команд и параметров технологического процесса: обнаружение команд управления контроллерным оборудованием (например, фактов подключения к контроллеру из инженерной среды, команд на включение и выключение, изменение прошивки, изменение текущей конфигурации) для следующих устройств:	
1.15.1.	- ABB AC 700F, 800M	Наличие
1.15.2.	- ABB AC 700F, 800M	Наличие
1.15.3.	- ABB B&R	Наличие
1.15.4.	- Allen-Bradley серий ControlLogix, CompactLogix	Наличие
1.15.5.	- AutomationDirect DirectLOGIC	Наличие
1.15.6.	- BECKHOFF серий CX	Наличие
1.15.7.	- Emerson DeltaV серий MD, MD Plus, MQ	Наличие
1.15.8.	- Emerson серии ControlWave	Наличие
1.15.9.	- General Electric RX3i	Наличие
1.15.10.	- Honeywell C300 для систем управления Experion PKS / PlantCruise	Наличие
1.15.11.	- Honeywell ControlEDGE серий 900	Наличие
1.15.12.	- IPU950	Наличие
1.15.13.	- Mitsubishi System Q E71	Наличие
1.15.14.	- OMRON серии CJ2M	Наличие
1.15.15.	- Schneider Electric Foxboro FCP270, FCP280	Наличие
1.15.16.	- Schneider Electric серии Modicon: M580, M340, Momentum	Наличие
1.15.17.	- Siemens SIMATIC серий S7-200, S7-300, S7-400, S7-1200, S7-1500	Наличие
1.15.18.	- YCU и ELC, поддерживающие протокол YARD	Наличие
1.15.19.	- Yokogawa CENTUM	Наличие
1.15.20.	- Yokogawa ProSafe-RS	Наличие
1.15.21.	- ОВЕН серий ПЛК100	Наличие
1.15.22.	- Прософт-Системы Regul R500	Наличие
1.15.23.	- Устройства KNX	Наличие
1.15.24.	- Устройства в системах управления Valmet DNA	Наличие
1.15.25.	- Устройства, поддерживающие протокол Allen-Bradley EtherNet/IP	Наличие
1.15.26.	- Устройства, поддерживающие протокол COS	Наличие
1.15.27.	- Устройства, поддерживающие протокол DTS	Наличие
1.15.28.	- Устройства, поддерживающие протокол FEU	Наличие
1.15.29.	- Устройства, поддерживающие протокол ПК4	Наличие
1.15.30.	- Устройства, поддерживающие протокол ПНУ20	Наличие
1.15.31.	- Устройства, поддерживающие протоколы CODESYS V2, V3	Наличие
1.15.32.	- Устройства, поддерживающие протоколы Siemens S7comm, S7comm-plus	Наличие
1.15.33.	- Устройства, поддерживающие протоколы стандарта PROFINET IO	Наличие
1.16.	Возможность мониторинга управляющих сетевых команд и параметров технологического процесса интеллектуальных электронных устройств (далее IED):	
1.16.1.	- ABB серии Relion: REF615, RED670, REL670, RET670	Наличие
1.16.2.	- General Electric серии Multilin: B30, C60	Наличие
1.16.3.	- MiCOM C264	Наличие
1.16.4.	- Schneider Electric P545	Наличие
1.16.5.	- Schneider Electric Sepam серии 80 NPP	Наличие
1.16.6.	- Siemens серии SIPROTEC 4: 6MD66, 7SA52, 7SJ64, 7SS52, 7UM62, 7UT63	Наличие
1.16.7.	- Релематика TOP 300	Наличие
1.16.8.	- ЭКРА серий 200, БЭ2502, БЭ2704	Наличие
1.16.9.	- устройства, поддерживающие протокол DNP3	Наличие
1.16.10.	- устройства, поддерживающие протокол Schneider Electric UMAS	Наличие
1.16.11.	- устройства, поддерживающие протоколы стандарта IEC 60870: IEC 60870-5-101, IEC 60870-5-104	Наличие
1.16.12.	- устройства, поддерживающие протоколы стандарта IEC 61850: IEC 61850-8-1 (GOOSE, MMS), IEC 61850-9-2 (Sampled Values)	Наличие
1.16.13.	- устройства, поддерживающие протокол Modbus TCP	Наличие
1.17.	Возможность мониторинга управляющих сетевых команд и параметров технологического процесса устройств с установленным серверным ПО:	

№ п/п	Наименование характеристики	Значение характеристики
1.17.1.	- FTP-сервер;	Наличие
1.17.2.	- сервер OPC DA;	Наличие
1.17.3.	- сервер OPC UA;	Наличие
1.17.4.	- сервер Siemens SICAM PAS;	Наличие
1.17.5.	- сервер TASE.2;	Наличие
1.17.6.	- сервер с поддержкой шифрования;	Наличие
1.17.7.	- устройства SCADA-системы АСРК	Наличие
1.18.	Возможность мониторинга управляющих сетевых команд и параметров технологического процесса устройств, относящихся к сетевому оборудованию:	
1.18.1.	- Моха серии NPort	Наличие
1.18.2.	- устройства ввода-вывода, поддерживающие протоколы BACnet, FTP, IEC 60870-5-101, IEC 60870-5-104, Modbus TCP, OPC DA, протокол взаимодействия устройств по технологии WMI, OPC UA Binary	Наличие
1.19.	Анализ параметров технологического процесса для оборудования и протоколов, указанных в пунктах 1.15.1-1.15.33, 1.16.1-1.16.13, 1.17.1-1.17.7, 1.18.1-1.18.2	Наличие
1.20.	Возможность обнаружения вторжений:	
1.20.1.	- обнаружение вредоносной активности и сетевых атак	Наличие
1.20.2.	- детектирование ARP Spoofing	Наличие
1.20.3.	- детектирование сканирования сети различными алгоритмами	Наличие
1.20.4.	- детектирование попыток перебора пароля	Наличие
1.20.5.	- детектирование атак типа «отказа в обслуживании»	Наличие
1.20.6.	- обновление базы сигнатур для выявления вредоносной активности	Наличие
1.21.	Возможность автоматического обнаружения уязвимостей промышленного оборудования на основании данных об атрибутах узлов (модель, производитель, версия программного и аппаратного обеспечения)	Наличие
1.22.	Возможность формирования инцидентов безопасности:	
1.22.1.	- Определение корреляции обнаруженных событий в контролируемых сегментах технологической сети	Наличие
1.22.2.	- Отображение обнаруженных инцидентов ИБ с помощью локального интерфейса специалиста ИБ	Наличие
1.23.	Возможность анализа инцидентов безопасности:	
1.23.1.	- Хранение архива трафика промышленной сети (в соответствии с настройками и ёмкостью диска)	Наличие
1.23.2.	- Хранение архива информации о событиях, обнаруженных в контролируемых сегментах сети	Наличие
1.23.3.	- Отправка инцидентов безопасности на сервер централизованного администрирования подсистем	Наличие
1.24.	Возможность отправки событий и инцидентов безопасности в системы класса SIEM с использованием протокола syslog/CEF	Наличие
1.25.	Возможность экспорта/импорта/очистки политики безопасности (конфигурации) решения	Наличие
1.26.	Поддержка графического Web-интерфейса с возможностью разграничения прав доступа для средства мониторинга технологических сетей.	Наличие
1.27.	Текстовые надписи Web-интерфейса средства мониторинга технологических сетей должны предусматривать отображение на русском и английском языках	Наличие
1.28.	Возможность аудита безопасности устройств путем проверки по встроенным и пользовательским наборам OVAL-описаний для:	
1.28.1.	- Анализа соответствия требованиям нормативной документации, включая Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости, приведенный в Приложении к Требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. N 239	Наличие
1.28.2.	- Анализа соответствия рекомендациям Разработчика ПО Системы в части общих настроек безопасности для ОС Windows, Linux и сетевого оборудования	Наличие
1.28.3.	- Поиска уязвимостей оборудования и ПО	Наличие
1.29.	Формирование отчетов с информацией о состоянии узлов и безопасности системы	Наличие
1.30.	Возможность контроля сегментов сети с одинаковыми адресами узлов	Наличие

№ п/п	Наименование характеристики	Значение характеристики
1.31.	Возможность вывода общей информации о защищенности технологической сети в формате виджетов на веб-интерфейсе:	
1.31.1.	- Устройства с состояниями безопасности – распределение устройств по их состояниям безопасности;	Наличие
1.31.2.	- Уценки событий – гистограмма распределения событий по значениям их оценок за выбранный период;	Наличие
1.31.3.	- События по технологиям – количественное распределение событий по технологиям регистрации событий за выбранный период;	Наличие
1.31.4.	- Частые пользователи программ в событиях – наиболее часто регистрируемые имена пользователей в событиях по данным от EPP-программ за выбранный период;	Наличие
1.31.5.	- Частые программы в событиях – наиболее часто регистрируемые сторонние программы в событиях по данным от EPP-программ за выбранный период;	Наличие
1.31.6.	- Частые устройства в событиях – наиболее часто регистрируемые устройства в событиях за выбранный период;	Наличие
1.31.7.	- Частые устройства по количеству рисков – наиболее часто регистрируемые устройства в обнаруженных рисках за выбранный период;	Наличие
1.31.8.	- Оценки рисков – гистограмма распределения рисков по значениям их оценок за выбранный период;	Наличие
1.31.9.	- Ситуационная осведомленность – уведомления о текущих выявленных угрозах для безопасности системы;	Наличие
1.31.10.	- Защищенность EPP-программами – количественное соотношение компьютеров, защищенных и не защищенных EPP-программами;	Наличие
1.31.11.	- Устройства – содержит информацию об устройствах в промышленной сети (используется распределение по категориям устройств);	Наличие
1.31.12.	- События – содержит информацию о событиях и инцидентах, имеющих наиболее поздние значения даты и времени последнего появления	Наличие
1.32.	Наличие сертификата ФСТЭК на ПО ПОВ на соответствие требованиям по безопасности информации средств защиты информации не ниже 5 класса защиты и 5 или более высокому уровню доверия на поставляемое ПО ПОВ, входящее в комплект поставки	№ 4027
1.33.	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.	Наличие
2.	<b>Лицензия на техническую поддержку программного обеспечения системы обнаружения вторжения, обновление баз и программных модулей для одного сервера - 1 шт.</b> <b>(KL4939RAAFS Kaspersky Industrial CyberSecurity for Networks Standard Server, Updates and Support, Enterprise Russian Edition. 1- Server 1 year Base License – Лицензия - 1 шт)</b>	-
2.1.	Срок действия лицензии	1 год
2.2.	Предоставление доступа к интернет-порталу технической поддержки круглосуточно, включая выходные и праздничные дни	Наличие
2.3.	Приём запросов по электронной почте в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни) в случае невозможности создания запроса через интернет-портал	Наличие
2.4.	Приём запросов по телефону приоритетной выделенной линии в режиме:	-
2.4.1.	- для запросов уровня критичности, означающего критическую проблему с ПО ПОВ, влияющую на непрерывность бизнеса, и уровня критичности, означающего проблему высокого уровня критичности, вызывающую воздействие на функциональность ПО ПОВ, но не вызывающую повреждение или потерю данных	круглосуточно

№ п/п	Наименование характеристики	Значение характеристики
2.4.2.	- для запросов других уровней критичности	По рабочим дням от 10:00 до 18:30 (время московское)
2.5.	Время реакции на инциденты:	-
2.5.1.	- для запросов уровня критичности, означающего критическую проблему с ПО ПОВ, влияющую на непрерывность бизнеса (в нерабочие дни необходимо обращение по телефону)	30 минут
2.5.2.	- для запросов уровня критичности, означающего проблему высокого уровня критичности, вызывающую воздействие на функциональность ПО ПОВ	4 ч
2.5.3.	- для запросов уровня критичности, означающего некритичную проблему или запрос на обслуживание, не затрагивающие функциональность ПО ПОВ	6 рабочих часов
2.5.4.	- для остальных запросов	8 рабочих часов

## 7.2 ТРЕБОВАНИЯ К ВНЕДРЕНИЮ ПОВ

### 7.2.1 ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ УСЛУГ

Исполнитель должен оказать услуги по внедрению программного обеспечения подсистемы обнаружения вторжений 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 ПОВ проводятся в соответствии с п. 3.2.3 и п. 3.3.3 «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 ПОВ Исполнитель должен проработать детальную конфигурацию ПОВ, перечень настроек, политик, актуализировать логические схемы взаимодействия, разработать программу и методику приемочных испытаний и согласовать проектные решения с Заказчиком.

В рамках внедрения ПОВ Исполнитель должен оказать следующие услуги:

1. Исполнитель должен осуществить поставку лицензий на ПО ПОВ с техническими характеристиками, приведенными в Таблице № 1.
2. Провести анализ имеющейся проектной документации на создание ПОВ (Приложение № 3 к Договору) и существующих бизнес-процессов Заказчика.
3. Проработать детальную конфигурацию ПОВ, 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 ПОВ КСОИБ ЗОКИИ Общества.
5. Разработать требования по подготовке инфраструктуры Заказчика для внедрения ПО ПОВ.
6. Выполнить установку и настройку операционной системы на подготовленные виртуальные серверы.
7. Выполнить установку и настройку ПО ПОВ на подготовленные виртуальные серверы.

8. Произвести настройку ПОВ на получение точного времени от находящегося в сегменте «Телескоп+» сервера времени.
9. Настроить интеграцию ПОВ со смежными системами.
10. Произвести обучение системы для определения разрешенных устройств, конфигураций и разрешающих правил.
11. Произвести настройку сетевого оборудования для передачи копии целевого трафика для анализа с использованием SPAN-портов.
12. Произвести настройку системы виртуализации для передачи копии целевого трафика к компонентам ПО ПОВ.
13. Предоставить Заказчику информацию по возможным отчетам, формируемым ПО ПОВ, и отображаемой в них информации. Разработать и настроить шаблоны отчетов.
14. Подготовить комплект документации техно-рабочего проекта.
15. Провести предварительные испытания.
16. Осуществить опытную эксплуатацию.
17. 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 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 выполнения таких работ должно согласовываться с Заказчиком. Предоставление технологических окон для выполнения работ 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, если это требуется в соответствии с законодательством РФ и/или положениями данного технического задания.

ПОВ 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 ПОВ для существующих на момент внедрения ПО ПОВ подсистем инфраструктуры ИТ, АРМ и серверов КСОИБ ЗОКИИ, АРМ и серверов ЗОКИИ, приборов учета. 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, приборов учета 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 выполнения всех работ.

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 ПОВ.

Выполнение работ/услуг по внедрению ПОВ может производиться дистанционно.

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

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

Архитектура ПОВ должна быть централизованной и состоять из сервера, который принимает данные, обрабатывает и предоставляет их пользователям, а также получает и анализирует данные из вычислительных сетей, подключенных к сетевым интерфейсам сервера.

ПОВ предназначена для анализа трафика с целью выявления отклонений в значениях технологических параметров, обнаружения признаков сетевых атак, контроля работы и текущего состояния устройств в сети.

ПОВ должна обеспечивать высокую производительность для решения возложенных задач, осуществлять одновременную работу нескольких пользователей, а также обладать высокой надежностью и отказоустойчивостью. ПОВ должна предусматривать возможность масштабирования по производительности и объему обрабатываемой информации путем модернизации используемого комплекса технических средств. Возможности масштабирования должны обеспечиваться средствами используемого базового программного обеспечения путем увеличения количества лицензий дополнительных компонентов получения и анализа трафика (сенсоров).

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

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

ПОВ должна обеспечивать возможность резервного копирования следующих данных ПО:

- политика безопасности;
- данные о состоянии и режимах работы технологий и методов;
- параметры обновления баз и программных модулей;
- информация о лицензионном ключе;
- записи аудита;
- сообщения программы;
- зарегистрированные события;
- сохраненный трафик для событий;
- данные карты сети;
- данные об исполняемых файлах.

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

Работа ПОВ 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 ПОВ 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 ПО ПОВ.

Для подключения к ПО ПОВ через веб-интерфейс должна быть обеспечена поддержка следующих браузеров:

- Google Chrome;
- Mozilla Firefox;
- Microsoft Edge;
- Chromium для Astra Linux.

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.

ПОВ должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях ПОВ 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. ПОВ 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

Перечень сетевых взаимодействий подсистемы обнаружения вторжений представлен в таблице №2.

Таблица №2

##### Перечень сетевых взаимодействий ПОВ

№	Компонент-источник	Система назначения	Протокол:Порт	Примечание
1.	АРМ управления СЗИ (ВМ)	Сервер управления Сенсор	SSH:22 HTTP:80 HTTPS:443	Управление
2.	Сервер управления	Сенсор	SSH:22 HTTP:80 HTTPS:443	Взаимодействие между компонентами системы

№	Компонент-источник	Система назначения	Протокол:Порт	Примечание
3.	Сервер управления	NTP-сервер	UDP:123	Синхронизация времени
4.	Сенсор	NTP-сервер	UDP:123	Синхронизация времени
5.	Сервер управления	Сервер мониторинга событий	TCP/UDP:514	Передача событий

Сетевые взаимодействия ПОВ уточняются при проектировании.

## 7.2.5 ТРЕБОВАНИЯ К НАДЕЖНОСТИ

ПОВ 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 ПОВ.

Программное обеспечение ПОВ 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 ПОВ должна обеспечиваться при следующих аварийных ситуациях:

- нарушения электропитания;
- нарушение или выход из строя канала связи;
- полный или частичный отказ серверов ПОВ, 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 ПОВ.

## 7.2.6 ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

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

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

Средства вычислительной техники ПОВ, 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 ПОВ.

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

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

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

В ПОВ должны выполняться требования к журналированию событий информационной безопасности. Срок хранения информации о событиях ИБ ПОВ 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 ПОВ должны использоваться защищенные протоколы с шифрованием (SSL, SFTP и т.п.).

Перед передачей ПОВ в опытно-промышленную и промышленную эксплуатацию должна быть проведена оценка соответствия ПОВ 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 ПОВ должны быть определены на этапе технического проектирования.

Средства используемых операционных систем должны обеспечивать документирование, протоколирование, хранение и управление 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 ПОВ 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>	Предельное значение скорости входящего трафика – не менее 500 Мбит/с.
<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 ПОВ. Срок хранения информации о событиях ИБ ПОВ в оперативном доступе должен составлять 1 год. В архивном доступе – 3 года с даты обнаружения события ИБ.
<b>ОЦЕНКА ОБЪЕМОВ ХРАНЕНИЯ ДАННЫХ</b>	Расчет дискового пространства должен быть произведен из необходимости хранения журналов событий не менее 3 месяцев

Требования должны быть уточнены на этапе проектирования.

## 7.2.9 ТРЕБОВАНИЯ К ОТЧЕТНОСТИ

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

Заказчик передает Исполнителю, ранее разработанную ПАО «Ростелеком» по договору с 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 ПОВ (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 ПОВ (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 ПОВ для существующих на момент внедрения ПОВ 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 ПОВ (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 ПОВ, 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 обеспечения функционирования ПО ПОВ.

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 ПОВ:

- Спецификация оборудования и программного обеспечения;
- Схема структурная;
- Пояснительная записка на создание ПОВ;
- Технический паспорт;
- Программа и методика предварительных испытаний;
- Программа опытной эксплуатации;
- Программа и методика приемочных испытаний;
- Руководство администратора;
- Руководство пользователя;
- Перечень созданных учетных записей и паролей ко всему поставленному и настроенному, системного и прикладному программному обеспечению;
- Инструкцию администратора, содержащую информацию о предварительной настройке АРМ и серверов для установки и обеспечения функционирования ПО ПОВ.

## 8 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ УСЛУГ

Контроль соответствия, разработанного в рамках данного проекта, функционала ПОВ 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 ПОВ устанавливаются следующие виды испытаний:

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

Испытания ПОВ 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 ПОВ 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 ПОВ 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 ПОВ 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 ПОВ в опытную эксплуатацию;
- 1.2. по результатам предварительных испытаний формируется Протокол, который должен содержать заключение о возможности (невозможности) приемки ПОВ в опытную эксплуатацию, а также перечень необходимых доработок и рекомендуемые сроки их выполнения;
- 1.3. предварительные испытания завершаются оформлением акта приемки ПОВ в опытную эксплуатацию.

### **2. Опытная эксплуатация:**

- 2.1. опытная эксплуатация ПОВ проводится с целью определения характеристик ПОВ и готовности персонала Заказчика к работе в реальных условиях

- функционирования ПОВ, а также определения фактической эффективности ПОВ и, при необходимости, корректировки документации;
- 2.2. по результатам опытной эксплуатации ПОВ принимается решение о возможности (невозможности) предъявления ПОВ на приемочные испытания.
- 2.3. опытная эксплуатация завершается оформлением акта о завершении опытной эксплуатации.
3. Приемочные испытания:
- 3.1. приемочные испытания ПОВ проводятся для определения соответствия ПОВ требованиям Технического задания, оценки качества опытной эксплуатации и решения вопроса о возможности ввода ПОВ в промышленную эксплуатацию;
- 3.2. приемочные испытания ПОВ 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 ПОВ требованиям настоящего ТЗ, и акт о готовности ПОВ 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 а 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 обнаружения вторжения (бессрочная базовая лицензия на право пользования основной функциональностью для одного сервера)	KL4935RAAZS Kaspersky Industrial CyberSecurity for Networks Standart Server Russian Edition. 1 – Server Base License – Лицензия Включая KL8069RMZZZ Kaspersky Certified media Pack Customized Russian	KL4935R AAZS	1 шт	5 526 033,08	5 526 033,08	5 526 033,08	НДС не облага ется	5 526 033,08	№ 8357 АО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"	58.29.12.0 00
2	Неисключительные права использования программного обеспечения системы обнаружения вторжения (базовая лицензия на обновление баз и программных модулей и техническую поддержку для одного сервера на 1 год)	KL4939RAAFS Kaspersky Industrial CyberSecurity for Networks Standart Server, Updates and Support, Enterprise Russian Edition. 1 – Server 1 year Base License – Лицензия	KL4939R AAFS	1 шт	3 868 223,39	3 868 223,39	3 868 223,39	НДС не облага ется	3 868 223,39	№ 8361 АО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"	58.29.12.0 00

3	Услуги по внедрению программного обеспечения системы обнаружения вторжения	-	-	1 условная единица	9 785 925,14	9 785 925,14	11 743 110,17	20	11 743 110,17	-	62.09.20.1 20
	ИТОГО:	x	x	x	x	19 180 181,61	x	x	21 137 366,64	x	x

- Итого стоимость по Спецификации составляет: 21 137 366 (Двадцать один миллион сто тридцать семь тысяч триста шестьдесят шесть) рублей 64 копейки, в том числе НДС в сумме 1 957 185 (Один миллион девятьсот пятьдесят семь тысяч сто восемьдесят пять) рублей 03 копейки, в том числе:
  - Стоимость Лицензий составляет: 9 394 256 (Девять миллионов триста девяносто четыре тысячи двести пятьдесят шесть рублей) рублей 47 копеек НДС не облагается на основании пп. 26 п. 2 ст. 149 НК РФ;
  - Стоимость Услуги составляет 11 743 110 (Одиннадцать миллионов семьсот сорок три тысячи сто десять рублей) рублей 17 копеек, в том числе НДС в сумме 1 957 185 (Один миллион девятьсот пятьдесят семь тысяч сто восемьдесят пять) рублей 03 копейки.
  - Конечный пользователь: ПАО «Самараэнерго»
  - Порядок предоставления Лицензий:
    - Передаются в электронном виде;
    - Передаются на электронную почту Заказчика: [info@samaraenergo.ru](mailto:info@samaraenergo.ru)
    - Условия предоставления Лицензий:
      - лицензии предоставляются в соответствии с общепринятым в мировой практике обычаем делового оборота – принципом «AS IS» («таким, каков он есть»).
  - Место передачи Лицензий и оказания Услуги:
  - по адресу места нахождения Заказчика: 443079, Российская Федерация, город Самара, проезд Георгия Митирева, дом 9
  - 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  
корпоративным и государственным 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

  
Р.Л. Шуман

М.П.

**Исполнитель:**

Заместитель директора филиала – директор по работе с корпоративным и государственным 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

«24» 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 обнаружения вторжения (далее – Лицензии) и оказания услуг по внедрению программного обеспечения системы обнаружения вторжения.

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)

### 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 408228103380000000002  
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.

**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

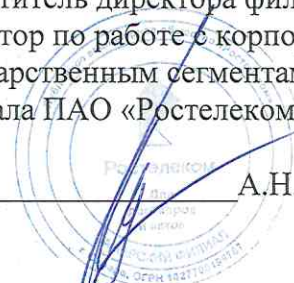


Р.Л. Шуман

М.П.

**Исполнитель:**

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



А.Н. Толочная

М.П.

**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



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.



## **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 указанным 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 личного 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



Р.Л. Шуман

М.П.

#### Исполнитель:

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



А.Н. Толочная

М.П.

