

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ №1 /649
к договору № 556 от 27.10.2025 г.

г. Самара

« 01 » 12 2025

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 настоящее Дополнительное соглашение к договору № 556 от 27.10.2025 г. (далее - «Соглашение») о нижеследующем.

1. Внести изменение в Приложение № 1 к Договору № 556 от 27.10.2025 г. и изложить его в редакции Приложения № 1 к Дополнительному соглашению к Договору № 556 от 27.10.2025 г.

2. Внести изменение в Приложение № 2 к Договору № 556 от 27.10.2025 г. и изложить его в редакции Приложения № 2 к Дополнительному соглашению к Договору № 556 от 27.10.2025 г. Спецификация.

3. Во всем остальном, что не предусмотрено настоящим Соглашением, Стороны руководствуются положениями Договора.

4. Настоящее Соглашение вступает в силу с момента подписания и распространяет своё действие на отношения Сторон на срок действия Договора № 556 от 27.10.2025 г.

5. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу для каждой из Сторон. Дополнительное соглашение является неотъемлемой частью Договора.

6. Список приложений:

6.1. Приложение № 1 к Дополнительному соглашению к Договору № 556 от 27.10.2025 г.

6.2. Приложение № 2 к Дополнительному соглашению к Договору № 556 от 27.10.2025 г.

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

А.Н. Толочная

МП



Заместитель генерального директора по техническим вопросам и информационным технологиям

Р.Л. Шуман



ТЕХНИЧЕСКОЕ ЗАДАНИЕ

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

**САМАРА
2025**

1 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

Термины и определения

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

№	ТЕРМИН	ОПРЕДЕЛЕНИЕ
		пользователей

Сокращения

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

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

2 ПРЕДМЕТ ЗАКУПКИ

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

3 ЦЕЛИ И РЕШАЕМЫЕ ЗАДАЧИ

Целью закупки является создание системы анализа защищенности информации для обеспечения защиты ИТ-инфраструктуры Общества, реализация мер по обеспечению информационной безопасности в рамках создания комплексной системы по обеспечению защиты ЗОКИИ Общества в соответствии с требованиями законодательства Российской Федерации, в том числе выполнение требований Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Федерации», обеспечение соответствия создаваемой инфраструктуры для ПО «Телескоп+» требованиям законодательства РФ в области обеспечения безопасности объектов критической информационный инфраструктуры, а также нейтрализации угроз информационной безопасности, реализация которых может привести к нарушению штатного режима функционирования ИС и управляемого (контролируемого) процесса, локализацию и минимизацию последствий от возможной реализации угроз безопасности информации, согласно пояснительной записки на создание КСОИБ ЗОКИИ Общества (02409271.26.20.40.140.139.П2) (Приложение № 3 к Договору).

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

Назначением внедряемой ПАЗИ является:

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

Для достижения поставленных целей Исполнителю требуется реализовать следующие задачи:

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

4 ПЛАНОВЫЕ СРОКИ НАЧАЛА И ОКОНЧАНИЯ УСЛУГ

Срок начала оказания услуг: с момента подписания договора.

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

5 МЕСТО ОКАЗАНИЯ УСЛУГ

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

6 ОБЩИЕ СВЕДЕНИЯ

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

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

6.1 ХАРАКТЕРИСТИКА ОБЪЕКТА ЗАЩИТЫ

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

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

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

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

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

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

6.2 КАТЕГОРИЯ ЗНАЧИМОСТИ ОБЪЕКТА КИИ

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

6.3 ПЕРЕЧЕНЬ ДОКУМЕНТОВ, НА ОСНОВАНИИ КОТОРЫХ ВНЕДРЯЕТСЯ ПАЗИ

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

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

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

6.4 РАЗДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ

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

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

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

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

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

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

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

Заказчик обеспечивает наличие и работоспособность защищенных каналов связи, защищенных волоконно-оптических линий связи либо наличие, работоспособность и

функционирование должным образом средств криптографической защиты информации в случае использования каналов связи, выходящих за пределы контролируемой зоны.

7 ОБЩИЕ ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ И ОКАЗАНИЮ УСЛУГ

7.1 ТРЕБОВАНИЯ К ПОСТАВЛЯЕМОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

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

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

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

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

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

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

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

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

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

Таблица № 1

№ п/п	Наименование характеристики	Значение характеристики
----------	-----------------------------	----------------------------

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

	<ul style="list-style-type: none"> - баз данных – Microsoft SQL, Oracle DB, Sybase, DB2, MySQL, PostgreSQL; - бизнес-приложений – SAP DIAG, SAP RFC; - сред виртуализации – VMware vSphere; - IP-телефонии – SIP 	
1.23.	<p>Поддержка справочников для сетевого сканирования:</p> <ul style="list-style-type: none"> - базовые заполненные справочники с парами «логин – пароль»; - пользовательские справочники для хранения пар «логин – пароль», справочники с логинами, справочники с паролями 	Да
1.24.	Поддержка возможности создания, изменения или удаления пользовательских справочников	Да
1.25.	Поддержка подключения к выбранным ИТ-активам по IP-адресам (подсетям), FQDN-именам или иным идентификаторам ИТ-активов	Да
1.26.	Поддержка выбора способов (протоколов) подключения к ИТ-активам и определения учетных записей, используемых для аутентификации	Да
1.27.	Поддержка механизма проверки доступности ИТ-активов для выполнения задач на сбор данных, в том числе поддержка проверки учетной записи, используемой при проверке доступности	Да
1.28.	<p>Обеспечение сбора инвентаризационной и конфигурационной информации путем сканирования ИТ-активов:</p> <ul style="list-style-type: none"> - идентификационных данных об ИТ-активах (IP-адрес, FQDN и другие); - данных о составе аппаратного обеспечения (материнская плата, центральный процессор, сетевая карта и другие); - данных о составе программного обеспечения (BIOS, ОС, общесистемное ПО и другие); - данных о настройках ОС семейства Windows (локальные и доменные политики); - данных о запущенных службах и задачах планировщика ОС. 	Да
1.29.	Поддержка сканирования узлов инфраструктуры (активов) методами белого и черного ящика.	Да
1.30.	Обеспечение автоматического выявления уязвимостей в соответствии с экспертной базой знаний на ИТ-активах с наличием информации достаточной для расчета уязвимостей	Да
1.31.	Обеспечение выявления уязвимостей в пакетах программ, вложенных в контейнеры, основанные на ОС семейства Linux, в том числе Debian и Ubuntu	Да
1.32.	Обеспечение модулями сбора данных, размещенными на технических средствах под управлением ОС семейства Linux возможности создания, изменения, удаления, запуска и приостановки задач поиска уязвимостей в веб-приложениях	Да
1.33.	Обеспечение отображения сведений об уязвимостях в виде карточки уязвимости, связанной с карточкой ИТ-актива	Да
1.34.	Отображение времени последнего сканирования ИТ-актива на наличие уязвимостей	Да
1.35.	<p>Обеспечение управления списком ИТ-активов, включая:</p> <ul style="list-style-type: none"> - поиск ИТ-активов по их атрибутам; - группировку ИТ-активов; - построение иерархии групп ИТ-активов; - поиск групп ИТ-активов по названию 	Да
1.36.	Поддержка группировки ИТ-активов в статические группы, членство ИТ-актива в которых определяется пользователем	Да
1.37.	Поддержка группировки ИТ-активов в динамические группы, членство в которых определяется ПО ПАЗИ автоматически на основе информации об ИТ-активе (IP-адреса, ОС, прочих характеристик)	Да
1.38.	<p>Обеспечение контроля ключевых показателей процесса управления ИТ-активами путем реализации настраиваемых политик и (или) правил, включая:</p> <ul style="list-style-type: none"> - активацию или деактивацию политики и (или) правила; - добавление, изменение или удаление политики и (или) правила 	Да
1.39.	Поддержка реализации политики и (или) правила определения и (или) изменения сроков актуальности и устаревания данных об активе	Да
1.40.	Поддержка реализации политики и (или) правила определения перечня активов, в отношении которых действует политика и (или) правило	Да
1.41.	Поддержка реализации политики и (или) правила присвоения значимости ИТ-активам	Да
1.42.	Обеспечение выполнения над ИТ-активом действий, описанных в политике и (или) правиле (при ИТ-активации политики и (или) правила)	Да
1.43.	Обеспечение возвращения состояния ИТ-актива в исходное при деактивации	Да

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

	2) определение перечня уязвимостей, в отношении которых действует правило; 3) определение перечня активов, в отношении которых действует правило	
1.58.	Обеспечение контроля ключевых показателей процесса управления уязвимостями путем реализации настраиваемых политик и (или) правил, включая: - активацию и (или) деактивацию политики и (или) правила; - добавление и (или) изменение и (или) удаление политики и (или) правила	Да
1.59.	Поддержка операций над сведениями об уязвимостях: - выделение важных (критических) уязвимостей; - контроль выполнения работ по устранению уязвимостей; - градация уязвимостей, в том числе выявление трендовых уязвимостей, то есть уязвимостей, которые активно используются в атаках злоумышленников в актуальный период времени (при условии постоянных обновлений базы знаний)	Да
1.60.	Поддержка операций управления обработкой уязвимостей: - поиск и сортировка уязвимостей по их атрибутам; - создание и (или) удаление информации (меток) к уязвимостям; - демонстрация карточек уязвимостей, содержащих справочную информацию в развернутом виде; - изменение статуса уязвимости; - контроль устранения уязвимостей; - проведение массовых операций над уязвимостями	Да
1.61.	Поддержка поиска по активам и уязвимостям с применением технологии искусственного интеллекта на русском и английском языках	Да
1.62.	Обеспечение ведения истории изменения уязвимостей с привязкой к конкретному активу, с отображением: - наличия уязвимости; - статуса уязвимости на заданный момент времени	Да
1.63.	Наличие предустановленного набора стандартов	Да
1.64.	Обеспечение проверки соответствия и принятие решений о соответствии текущих параметров программных и программно-технических средств (ИТ-активов) требованиям предустановленных в ПО ПАЗИ технических стандартов	Да
1.65.	Поддержка возможности импорта пользовательских стандартов в формате YAML	Да
1.66.	Поддержка возможности импорта пользовательских требований	Да
1.67.	Поддержка механизма валидации импортируемых требований	Да
1.68.	Обеспечение валидации требований, существующих в ПО ПАЗИ (при внесении изменений, влияющих на работу требования)	Да
1.69.	Обеспечение отображения критичности требований в стандарте (по уровню опасности)	Да
1.70.	Поддержка возможности установки пользовательских меток на конкретные требования	Да
1.71.	Поддержка возможности указания для каждого импортируемого стандарта следующих параметров: - идентификатор стандарта; - отображаемое имя стандарта; - текстовое описание стандарта; - название регламентирующего документа, на основании которого создан стандарт; - параметры привязки узлов ИТ-актива к требованию; - требования, входящие в стандарт; - новые значения параметров требований (при необходимости)	Да
1.72.	Поддержка возможности создания политик и (или) правил проверки соответствия стандартам	Да
1.73.	Поддержка возможности присвоения статусов ИТ-активам, не соответствующим стандартам	Да
1.74.	Поддержка возможности создания политик и (или) правил устранения несоответствия ИТ-актива стандарту	Да
1.75.	Поддержка возможности просмотра оценки соответствия ИТ-актива стандарту (по результатам его проверки правилом проверки соответствия)	Да
1.76.	Обеспечение хранения данных, содержащих выявленные в различные моменты времени сведения об ИТ-активах, в том числе IP-адреса, доменные имена и	Да

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

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

7.2 ТРЕБОВАНИЯ К ВНЕДРЕНИЮ ПАЗИ

7.2.1 ТРЕБОВАНИЯ К ОКАЗАНИЮ УСЛУГ

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

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

Перед началом оказания услуг по внедрению ПАЗИ Исполнитель должен проработать детальную конфигурацию ПАЗИ, перечень настроек, политик, актуализировать логические

схемы взаимодействия, разработать программу и методику приемочных испытаний и согласовать проектные решения с Заказчиком.

В рамках внедрения ПАЗИ Исполнитель должен оказать следующие услуги:

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

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

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

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

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

Специалисты Исполнителя должны обладать необходимыми для выполнения работ/услуг компетенциями и опытом, иметь необходимые сертификаты на проведение работ/услуг, если это требуется в соответствии с законодательством РФ и/или положениями данного технического задания.

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

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

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

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

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

Выполнение работ/услуг по внедрению ПАЗИ может производиться дистанционно.

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

7.2.2 ТРЕБОВАНИЯ К ПАЗИ И ЕЁ ФУНКЦИЯМ

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

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

ПАЗИ должна обеспечивать высокую производительность для решения возложенных задач, осуществлять одновременную работу нескольких пользователей, а также обладать высокой надежностью и отказоустойчивостью. ПАЗИ должна предусматривать возможность

масштабирования по производительности и объему обрабатываемой информации без модификации ее программного обеспечения путем модернизации используемого комплекса технических средств. Возможности масштабирования должны обеспечиваться средствами используемого базового программного обеспечения.

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

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

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

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

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

7.2.3 ТРЕБОВАНИЯ К ПОЛЬЗОВАТЕЛЬСКОМУ ИНТЕРФЕЙСУ

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

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

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

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

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

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

Экранные формы должны проектироваться с учётом требований унификации:

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

7.2.4 РЕШЕНИЯ ПО ВЗАИМОСВЯЗЯМ СИСТЕМЫ

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

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

Таблица №2

Перечень сетевых взаимодействий ПАЗИ

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

Сетевые взаимодействия ПАЗИ уточняются при проектировании.

7.2.5 ТРЕБОВАНИЯ К НАДЕЖНОСТИ

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

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

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

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

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

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

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

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

Сохранность информации в ПАЗИ должна обеспечиваться при следующих аварийных ситуациях:

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

7.2.6 ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

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

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

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

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

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

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

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

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

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

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

Перед передачей ПАЗИ в опытно-промышленную и промышленную эксплуатацию должна быть проведена оценка соответствия ПАЗИ требованиям информационной

безопасности путем проведения соответствующих испытаний согласно ПиМИ, направленных на проверку выполнения указанных в проектной документации и данном техническом задании мер безопасности.

Требования информационной безопасности могут быть уточнены на этапе технического проектирования.

7.2.7 ТРЕБОВАНИЯ К ИНФОРМАЦИОННОМУ ОБЕСПЕЧЕНИЮ

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

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

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

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

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

7.2.8 ТРЕБОВАНИЯ К ДОСТУПНОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ

Таблица №3

Требования к доступности и производительности

РЕЖИМ РАБОТЫ СИСТЕМЫ	Предполагаемый режим работы системы 24x7
МАКСИМАЛЬНОЕ ВРЕМЯ ВОССТАНОВЛЕНИЯ ПОСЛЕ СБОЯ И МАКСИМАЛЬНОЕ ОКНО ПОТЕРИ ДАННЫХ	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.
НАГРУЗКА	Максимальное количество сканируемых и контролируемых активов - не менее 250.
ТРЕБОВАНИЯ К РЕЗЕРВНОМУ КОПИРОВАНИЮ И ВОССТАНОВЛЕНИЮ	Должны быть предусмотрены средства резервного копирования и восстановления данных и конфигураций. Резервированию подлежат следующие типы данных: - журналы с внутренними событиями ОС и СУБД; - параметры функционирования модулей подсистем ПАЗИ. Срок хранения информации о событиях ИБ ПАЗИ в оперативном доступе должен составлять 1 год. В архивном доступе – 3 года с даты обнаружения события ИБ.

7.2.9 ТРЕБОВАНИЯ К ОТЧЕТНОСТИ

ПАЗИ должна предоставлять:

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

7.3 ПОДГОТОВКА КОМПЛЕКТА ДОКУМЕНТАЦИИ

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

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

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

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

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

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

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

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

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

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

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

- ☐ руководство администратора;
- ☐ руководство пользователя.

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

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

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

Комплект документов следует передавать с соблюдением требований сохранения конфиденциальности информации.

Состав передаваемой Заказчику документации ПАЗИ:

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

- ☐ Программа и методика приемочных испытаний;
- ☐ Руководство администратора;
- ☐ Руководство пользователя.

8 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ УСЛУГ

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

Для ПАЗИ устанавливаются следующие виды испытаний:

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

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

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

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

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

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

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

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

1. Предварительные испытания:

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

2. Опытная эксплуатация:

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

3. Приемочные испытания:

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

Заместитель генерального директора по
техническим вопросам и
информационным технологиям

Р.Л. Шуман

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

А.Н. Толочная

Спецификация

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

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

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

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

2. Конечный пользователь: ПАО «Самараэнерго»

3. Порядок предоставления Лицензий:

☐ Передаются в электронном виде;

☐ Предаются на электронную почту Заказчика: info@samaraenergo.ru

4. Условия предоставления Лицензий:

☐ лицензии предоставляются в соответствии с общепринятым в мировой практике обычаем делового оборота – принципом «AS IS» («таким, каков он есть»).

5. Место передачи Лицензий и оказания Услуг:

☐ по адресу места нахождения Заказчика: 443079, Российская Федерация, город Самара, проезд Георгия Митирева, дом 9

6. Место предоставления документов:

☐ по адресу места нахождения Заказчика: 443079, Российская Федерация, город Самара, проезд Георгия Митирева, дом 9

Заказчик

Заместитель генерального директора
по техническим вопросам и
информационным технологиям



М. П.

Д. Шуман

Исполнитель

Заместитель директора филиала – директор по работе с
корпоративным и

государственным сегментами Самарского
филиала ПАО «Ростелеком»



А.Н. Толочная