АНО Цифровой аудит

115114, город Москва, ул. Летниковская, д. 2, стр. 3, помещение 1
ИНН: 9704252434, КПП: 770501001, ОГРН: 1247700704877
E-mail: info@da.gov.ru, https://da.gov.ru

От 17.02.2026 № 39-УЗ/26

Руководителю организации

ЗАПРОС О ПРЕДОСТАВЛЕНИИ ЦЕНОВОЙ ИНФОРМАЦИИ

Автономная некоммерческая организация «Цифровой аудит» (далее – АНО «Цифровой аудит») планирует провести закупку права использования программного обеспечения платформы управления контейнеризацией (далее – ПО) на условиях простой (неисключительной) лицензии в соответствии с Техническим заданием (приложение № 1).

Предполагаемые сроки проведения закупки: февраль 2026 года.

Просим предоставить информацию о ценах и условиях предоставления прав, указанных в Техническом задании, по форме, предусмотренной приложением № 2.

Предложение должно содержать: срок действия предлагаемой цены; расчет цены, включая любые расходы, затраты и вознаграждения в связи с исполнением договора; цену за единицу лицензии, общую стоимость договора на условиях, указанных в Техническом задании.

Предоставленная информация должна быть заверена подписью лица, ответственного за предоставляемую информацию в соответствии с принятым в организации порядком подписания документов, содержащих ценовую информацию и условия исполнения принятых в соответствии с данной ценовой информацией обязательств и подтверждена печатью организации в случае ее наличия. Ответственность за недостоверность информации в КП и (или) документов, включенных в КП, за действия, совершенные на основании указанных информации и(или) документов, несет организация, предоставившая КП.

Ответ прошу направить с использованием электронной торговой площадки или на адрес электронной почты: zakupki_ano@da.gov.ru в срок, указанный в запросе на электронной торговой площадке.

Обращаем Ваше внимание, что настоящий запрос направлен исключительно с целью сбора информации о стоимости закупки, не является извещением о проведении закупки, офертой или публичной офертой и не влечет за собой возникновения каких-либо обязательств для сторон.

Приложения:

1. Приложение № 1 Техническое задание на 8 л.;
2. Приложение № 2 Форма предоставления коммерческого предложения на 1 л.

Руководитель Управления закупок **Ю.С. Пыленок**

М.В. Жигунова

Приложение 1
Техническое задание

Техническое задание на предоставление права использования программного обеспечения платформы управления контейнеризацией на условиях простой (неисключительной) лицензии

1. Термины и определения

Лицензиат	Автономная некоммерческая организация «Цифровой аудит»
Лицензиар	Организация, предоставляющая Лицензиату неисключительное право на использование программного обеспечения
Конечный пользователь, СП РФ, Сублицензиат	Счетная палата Российской Федерации, ИНН: 7702166610; КПП: 770401001
ИТ	Информационные технологии
ГИС ЕЦП ЦА	1-я очередь государственной информационной системы «Единая цифровая платформа «Цифровой аудит» Счетной палаты Российской Федерации»
ТЗ	Настоящее Техническое задание
ПО, Платформа	Программное обеспечение платформы управления контейнеризацией
ГК	Государственный контракт от 30 мая 2025 г. № 19д-25-3609

2. Функциональные требования.

2.1 Назначение:

Платформа предназначена для управления приложениями и их зависимостями в изолированных средах, называемых контейнерами.

2.2 Требования к функциональности ПО:

- обеспечение автоматизации и управления жизненным циклом контейнеров;
- поддержка процессов развертывания контейнеров с собранными внутри приложениями;
- поддержка декларативного управления кластером;
- предоставление инструментов для создания, развертывания, запуска и управления приложениями в контейнерной среде;
- предоставление инструментов управления кластером, развертываниями и другими ресурсами;
- предоставление встроенных средств планирования ресурсов кластера и балансировки нагрузки;
- предоставление механизмов ролевого доступа к ресурсам кластера.

В состав платформы должны входить следующие компоненты:

- Компоненты управляющего слоя (мастер-узел) — отвечают за основные операции кластера, а также обрабатывают события кластера (управляющий узел);
- Компоненты узла (рабочий узел) — работают на каждом узле, на котором разворачиваются контейнеризованные приложения, поддерживая работу группы контейнеров среды выполнения.

2.2.1 Дополнительные требования к ПО:

- Платформа должна иметь возможность установки на любую аппаратную платформу на базе процессорной архитектуры x86-64, вне зависимости от вендора или конкретной реализации аппаратного обеспечения.
- Дистрибутив ПО не должен требовать связи с сетью «Интернет» для установки;
- Обновление дистрибутива ПО должно представлять собой завершённый набор файлов, который может быть загружен в ГИС и установлен без доступа к сети «Интернет»
- Платформа должна предоставлять возможности распределения вычислительной нагрузки между сервисами.
- Платформа должна предоставлять сервис по масштабированию вычислительных ресурсов для обеспечения работы сервисов, без необходимости выгрузки-загрузки данных или прерывания доступа к сервисам.
- Платформа должна балансировать сетевой трафик между сервисами.
- Платформа должна обеспечивать единый комплекс и единую точку развертывания и мониторинга работоспособности сервисов.
- Платформа должна обеспечивать автоматизированную загрузку образов и дистрибутивов программного обеспечения указанных сервисов.
- Платформа должна обеспечивать изоляцию основного рабочего контура от доступа из внешней

сети, с контролируемым доступом к сервисам.

−Платформа должна обеспечивать автоматизированный контроль целостности и версий дистрибутивов и релизов сервисов, с возможностью загрузки и инсталляции таковых из доверенных источников (реестров).

−Платформа должна предоставлять наличие интеграционных модулей для основных инструментов сборки и интеграции ПО, совместимых с продуктами на основе Ansible, Terraform, Jenkins, Gitlab, GitlabCI, Репозитории пакетов и библиотек.

−Платформа должна предоставлять наличие функционала диагностирования проблем при запуске и загрузке контейнера, включая сбор и предоставление диагностической информации в процессе загрузки контейнера.

−В платформе должна присутствовать проверка стандарту CIS benchmark.

−Платформа должна обеспечивать поддержку отказоустойчивой архитектуры;

−Платформа должна обеспечивать возможность работы в закрытых контурах без доступа к сети интернет;

−Платформа должна обеспечивать возможность установки продукта как на физических, так и на виртуальных машинах;

−Платформа должна обеспечивать настройку квот на использование ресурсов CPU/RAM/Storage для Пространств имен (Namespace) и Узлов (Node);

−Платформа должна обеспечивать отправку событий мониторинга по настраиваемым триггерам во внешние системы (Grafana, Prometheus);

−Платформа должна иметь предварительно настроенный CNI (Container Network Interface);

−Платформа должна иметь оркестрацию контейнеров — процесс автоматизации конфигурирования, компоновки и управления контейнерами, позволяющий развертывать приложения в требуемом масштабе с заданными ресурсами;

−Платформа должна иметь функционал балансировки нагрузки — распределение трафика для обеспечения стабильности, обнаружения и связывание между собой контейнерных приложений с использованием DNS имени или своего собственного IP-адреса;

−Платформа должна иметь функционал автоматического масштабирования — масштабирование приложений на основе нагрузки процессора или других метрик, определенных пользователем;

−Платформа должна иметь функционал управления конфигурациями без переразвертывания контейнера;

−Система оркестрации должна содержать инструмент автоматического создания и обновления сертификатов для организации цепочки доверия без доступов в сеть интернет;

−Оркестратор должен поддерживать автоматическую установку контейнерного сетевого интерфейса при создании кластеров;

−Пользователям оркестратора должны быть доступны как минимум 2 типа контейнерных сетевых интерфейсов:

- легковесный, обеспечивающий сетевое взаимодействие между подами. Работает на уровне L3. Не обеспечивает безопасность соединения, а отвечает за корректное соединение между узлами кластера и подами;
- полнофункциональный. Данное решение обеспечивает надежное и безопасное сетевое соединение для подов кластеров. Работает на уровне L3/L4. Внедряет защищенную сеть для общения между подами кластера. Должны быть возможность выбора плана работы: iptables, eBPF;

−После создания кластера все его узлы должны иметь сетевую связанность согласно выбранному контейнерному сетевому интерфейсу;

−Оркестратор должен предоставлять возможность включения аудирования в API server, разворачиваемых кластеров, через WEB интерфейс;

−Автомасштабирование должно отслеживать метрику загрузки CPU, получаемую непосредственно от пода кластера. Должна быть реализована возможность настройки порогового значения срабатывания автомасштабирования;

−Вместе с оркестратором должен поставляться встроенный сервер для присвоения доменных имён, который позволяет получить доступ к WEB интерфейсу оркестратора в закрытых контурах, без доступа в интернет;

−В комплект поставки оркестратора должны включаться агенты контроля, осуществляющие контроль и настройку зависимостей устанавливаемых приложений;

−В платформе должен быть реализован веб интерфейс для настройки и развертывания контейнеризированных сред;

−В комплект поставки оркестратора должна входить утилита, обеспечивающая настройку балансировщиков нагрузки с рабочей нагрузкой, размещенной в кластере;

−Автоматизация развертывания:

- поддержка малой вариативности (работа с предустановленными настройками);
- наличие средства построения типовых инфраструктур;
- Наблюдаемость системы:
  - наличие журнала безопасности;
  - уведомление о событиях;
  - поддержка настройки сетевых политик;

- Платформа должна обеспечивать функциональные возможности, документально подтвержденные сертификатом ФСТЭК России:
  - уровню доверия средства контейнеризации;
  - хостовой операционной системе, в среде которой функционирует средство контейнеризации;
  - составу функций безопасности средства контейнеризации;
  - изоляции контейнеров средством контейнеризации;
  - выявлению уязвимостей в образах контейнеров;
  - проверке корректности конфигурации контейнеров;
  - контролю целостности контейнеров и их образов в средстве контейнеризации;
  - регистрации событий безопасности в средстве контейнеризации;
  - управлению доступом в средстве контейнеризации;
  - идентификации и аутентификации пользователей в средстве контейнеризации;
- Средство контейнеризации дополнительно должно реализовывать следующие механизмы:
  - изоляция пространств идентификаторов процессов контейнеров;
  - изоляция пространств имен для межпроцессного взаимодействия контейнеров;
  - изоляция пространств имен для пользователей и групп контейнеров;
  - изоляция пространств имен хостов и доменов контейнеров;
  - изоляция сетевых пространств имен контейнеров;
  - изоляция пространств имен для иерархии каталогов контейнеров.

- К выявлению уязвимостей в образах контейнеров предъявляются следующие требования:
  - Средство контейнеризации должно:
    - выявлять известные уязвимости при создании, установке образа контейнера в информационной (автоматизированной) системе и хранении образов контейнеров во взаимодействии с сертифицированным средством контроля и анализа защищенности на основе сведений, содержащихся в банке данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541), а также в иных источниках, содержащих сведения об известных уязвимостях;
    - оповещать о выявленных уязвимостях в образах контейнеров разработчика образов контейнеров и администратора безопасности информационной (автоматизированной) системы.
  - Средство контейнеризации должно осуществлять выявление известных уязвимостей образов контейнеров не реже одного раза в месяц.
  - Средство контейнеризации должно запрещать создание образов контейнеров, содержащих известные уязвимости критического и высокого уровня опасности.
  - Средство контейнеризации должно осуществлять выявление известных уязвимостей образов контейнеров не реже одного раза в неделю.
- К проверке корректности конфигурации контейнеров в средстве контейнеризации предъявляются следующие требования:
  - Средство контейнеризации должно обеспечивать возможность:
    - ограничение прав прикладного программного обеспечения, выполняемого внутри контейнера, на использование периферийных устройств, устройств хранения данных и съемных машинных носителей информации (блочных устройств), входящих в состав информационной (автоматизированной) системы;
    - ограничение прав прикладного программного обеспечения, выполняемого внутри контейнера, на использование вычислительных ресурсов (оперативной памяти, операций ввода-вывода за период времени) хостовой операционной системы;
    - монтирование корневой файловой системы хостовой операционной системы в режиме "только для чтения".

- Контроль целостности в средстве контейнеризации должен обеспечивать:
    - контроль самостоятельно или с применением средств контроля целостности хостовой операционной системы и иных сертифицированных средств защиты информации целостности образов контейнеров и исполняемых файлов контейнеров;
    - информирование администратора информационной (автоматизированной) системы и администратора безопасности средства контейнеризации о нарушении целостности объектов контроля
    - контроль целостности параметров настройки средства контейнеризации
    - контроль целостности сведений о событиях безопасности самостоятельно или во взаимодействии с хостовой операционной системой и иными сертифицированными средствами защиты информации;
    - контроль целостности образов контейнеров и параметров настройки средства контейнеризации при установке образа контейнера в информационной (автоматизированной) системе и далее периодически за счет применения цифровой подписи самостоятельно или во взаимодействии с хостовой операционной системой и иными сертифицированными средствами защиты информации;
    - блокировать запуск образа контейнера при нарушении его целостности.
- Регистрация событий безопасности в средстве контейнеризации должна позволять:
    - регистрировать события, относящиеся к инцидентам безопасности средства контейнеризации, связанные с попытками осуществления несанкционированного доступа к средству контейнеризации;
    - оповещать администратора безопасности средства контейнеризации и администратора информационной (автоматизированной) системы об инцидентах безопасности;
    - выполнять действия, являющиеся реакцией на инциденты безопасности;
    - осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
    - регистрировать следующие события безопасности (описание события безопасности и сведения о критичности события безопасности):
        - выявление известных уязвимостей в образах контейнеров и некорректности конфигурации;
        - факты нарушения целостности объектов контроля.
        - запись событий безопасности контейнеров в журнал событий безопасности информационной (автоматизированной) системы с указанием идентификатора пользователя хостовой операционной системы, от имени которого был запущен контейнер.
- Регистрация событий безопасности в средстве контейнеризации должна осуществляться с учетом требований разделов 5-6 ГОСТ Р 59548-2022 "Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации".
- Для каждой функции безопасности в средстве контейнеризации должен быть определен перечень событий, необходимых для регистрации и учета.
- Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны указываться номер (уникальный идентификатор) события, дата, время, тип события безопасности.
- Записи журнала событий безопасности должны представляться в структурированном виде и содержать информацию о времени события безопасности, взятую из хостовой операционной системы.
- Средство контейнеризации должно осуществлять запись событий безопасности контейнеров в журнал событий безопасности информационной (автоматизированной) системы с указанием идентификатора контейнера.
- Журнал событий безопасности средства контейнеризации должен быть доступен только для чтения. При исчерпании области памяти, отведенной под журнал событий безопасности средства контейнеризации, средство контейнеризации должно осуществлять архивирование журнала с последующей очисткой указанного журнала.
- Регистрации подлежат как минимум следующие события безопасности:
    - неуспешные попытки аутентификации пользователей средства контейнеризации;
    - создание, модификация и удаление образов контейнеров;
    - получение доступа к образам контейнеров;
    - запуск и остановка контейнеров с указанием причины остановки.
    - изменение ролевой модели;
    - модификация запускаемых контейнеров.

- Требования к управлению доступом в средстве контейнеризации.
- В средстве контейнеризации должен быть реализован ролевой метод управления доступом с тремя ролями пользователей:
    - разработчик образов контейнеров;
    - администратор безопасности средства контейнеризации;
    - администратор информационной (автоматизированной) системы.
- Роль разработчика образов контейнеров должна позволять:
    - менять установленный администратором безопасности средства контейнеризации для разработчика пароль;
    - создавать, модифицировать и удалять образы контейнеров.
- Роль администратора информационной (автоматизированной) системы должна позволять:
    - менять установленный администратором безопасности средства контейнеризации для администратора информационной (автоматизированной) системы пароль;
    - запускать и останавливать контейнеры.
- Роль администратора безопасности средства контейнеризации должна позволять:
    - назначать права доступа пользователям средства контейнеризации к образам контейнеров;
    - создавать учетные записи пользователей средства контейнеризации;
    - управлять учетными записями пользователей средства контейнеризации;
    - иметь доступ на чтение к журналу событий безопасности средства контейнеризации;
    - формировать отчеты с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности средства контейнеризации

- Требования по безопасности:
    - Платформа должна функционировать в среде сертифицированной операционной системы. Средство контейнеризации 4 класса защиты должно функционировать в среде хостовой операционной системы, соответствующей 4 классу защиты и 4 уровню доверия.

2.3 Требования к сертификации:

- ПО должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации.
- ПО должно соответствовать требованиям по безопасности информации, установленным в документах ФСТЭК России:
    - «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» - не ниже, чем по 4 уровню доверия;
    - «Требования по безопасности информации к средствам контейнеризации» - не ниже, чем по 4 классу защиты.
- ПО должно быть применимо для:
    - для создания государственных информационных систем до 1 класса защищенности включительно в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденными приказом ФСТЭК России от 11.04.2025 г. №117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (далее – приказ ФСТЭК России №117);
    - для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных не ниже 2 уровня защищенности, в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Условия лицензирования ПО.

3.1. Лицензиар обязуется предоставить на условиях простой (неисключительной) лицензии право использования ПО в соответствии с требованиями ТЗ на срок действия исключительных прав (бессрочно).

3.2. Право использования, предоставляемое Лицензиату, включает право использовать ПО (в том числе исправления ПО (patches), обновления ПО (upgrade) и обновленные версии ПО (updates)) на территории Российской Федерации следующими способами:

– установка ПО;

– воспроизведение ПО;

– распространение (передача) прав на ПО третьим лицам (конечному пользователю) в пределах всех прав Лицензиата.

–осуществление прав пользователя в порядке ст. 1280 ГК РФ;

Лицензиар предоставляет гарантию, что функциональность каждой самостоятельной версии ПО (в том числе исправления ПО (patches), обновления ПО (upgrade) и обновленные версии ПО (updates)) не зависит от последующих обновлений, не влияет на работоспособность установленной версии ПО.

Лицензиат вправе использовать ПО (в том числе исправления ПО (patches), обновления ПО (upgrade) и обновленные версии ПО (updates)) в целях оказания услуг Сублицензиату.

Лицензиат вправе использовать ПО (в том числе исправления ПО (patches), обновления ПО (upgrade) и обновленные версии ПО (updates)) в рамках исполнения обязательств по государственным контрактам (договорам), заключенным с Сублицензиатом.

Сублицензиат имеет право использовать ПО, в том числе исправления ПО (patches), обновления ПО (upgrade) и обновленные версии ПО (updates) в рамках функционирования и модернизации (развития) ГИС ЕЦП ЦА в объеме, не ограничивающем права СП РФ, в том числе на передачу, развитие ГИС ЕЦП ЦА.

Также Лицензиар предоставляет гарантии и заверения в отношении ПО, что ПО подвергалось тестированию в объеме:

- статический анализ;
- анализ заимствованных компонентов;
- динамический анализ, включая фаззинг-тестирование;
- функциональное тестирование;

нефункциональное тестирование (тестирование на проникновение).

Условия лицензирования ПО:

Тип ПО	Тип сервера	Количество серверов	Кол-во ядер на сервер (шт.)	Объем ОЗУ на сервер (ГБ)
Платформа управления контейнеризацией	Сервер «Узел управления» в открытом контуре	3	2x4	24
	Сервер «Рабочий узел» в открытом контуре	3	2x24	256
	Сервер «Узел управления» в закрытом контуре	3	2x16	256
	Сервер «Рабочий узел» в Закрытом контуре	5	2x48	512

–Лицензия включает гарантийную поддержку до 31.12.2027 года включительно.

В рамках гарантийной поддержки предоставляется доступ к обновлениям ПО, в соответствии с перечнем приобретаемого ПО в течение срока действия гарантийной поддержки.

Условия гарантийной поддержки:

Описание инцидента	**Приоритет**	**Срок реакции на заявку**	**Срок решения проблемы**
Критическая ошибка Ошибка, которая приводит к остановке функционирования Системы	1 – высший	1 часа (1 отчет о статусе в день)	Не более 8 часов
Существенная ошибка Ошибка, которая может привести к нарушению функционирования Системы, но допускает временное альтернативное решение	2 – средний	2 часа (1 отчет о статусе в день)	Не более 2-ух рабочих дней
Несущественная ошибка Ошибка, которая может привести к несущественному нарушению функционированию Системы	3 – низкий	8 рабочих часов (1 отчет о статусе в день)	Не более 1 месяца

Описание сервисов гарантийной поддержки

- Коммуникация | Сервис:
  - Почта;
  - Выделенный канал коммуникации (Telegram/Max);
  - Оперативная онлайн-консультация в чате;
  - Выделенный Service Desk;
  - Выделенный менеджер сопровождения (CSM);
- Обработка инцидента | Запрос на улучшение продукта | Консультации по функционированию и настройке:
  - Запрос на дополнительную функцию (пожелание к продукту), сопоставление с технологическим развитием продукта;
  - Выделенный инженер для разбора задач в ежедневном режиме;
  - Оперативное исправление - подготовка решения вне обычного цикла обновлений, предназначенное для исправления ошибок;
- Доступ к программам обучения по продукту.

Прием обращений в режиме 24/7 (круглосуточно, включая выходные и праздничные дни).

• Уровень поддержки должен быть соблюден даже в случае отсутствия удаленного защищенного доступа до инсталляции в пределах МКАД; Лицензиат гарантирует возможность предоставления доступа к оборудованию с Платформой или до автоматизированного рабочего места с таковым доступом 24x7x365 для обеспечения уровня поддержки;

• Приоритет заявки определяется Лицензиатом, пересмотр приоритета допускается только по согласованию с Лицензиатом;

• Сервисы гарантийной поддержки предоставляются на срок до 31.12.2027 и включены в стоимость лицензии.

4. Требования к безопасности ПО

Лицензиар гарантирует, что ПО отвечает требованиям о защите информации, установленным приказом ФСТЭК России № 117.

Лицензиар обязуется устранить уязвимости критического и высокого уровня опасности в соответствии с положениями соответствующих приказов Федеральной службы по техническому и экспортному контролю России и Федеральной службы безопасности России или предложить компенсирующие меры:

• в отношении уязвимостей критического уровня опасности - в срок не более 24 часов;

• в отношении уязвимостей высокого уровня опасности - в срок не более 7 календарных дней,

в случае, если такие уязвимости обнаружены Сублицензиатом/Лицензиатом в ПО, право использования которого передается в рамках договора, в срок до 31.12.2027 в процессе установки/настройки/интеграции ПО и до момента передачи результатов работ по ГК.

5. Срок и условия предоставления права использования ПО

5.1. Право использования ПО считается предоставленным Лицензиату с даты подписания Сторонами акта на предоставление права использования программного обеспечения на условиях простой (неисключительной) лицензии (далее – Акт).

5.2. Лицензиар в течение 5 (Пяти) рабочих дней с даты заключения Договора, но не позднее 16.03.2026, передает Лицензиату по адресу: г. Москва, ул. Летниковская, д. 2, стр. 3, подписанный и заверенный оттиском печати со своей стороны Акт в 2 (Двух) экземплярах.

5.3. Не позднее даты передачи Акта и в месте его передачи Лицензиар должен передать Лицензиату документ на бумажном носителе, содержащий состав лицензии ПО и лицензионный ключ для активации ПО.

5.4. Сублицензиат/Лицензиат не обязаны предоставлять Лицензиару отчеты об использовании ПО.

6. Приемка права использования ПО

6.1. Лицензиат не позднее 30.10.2026 осуществляет приемку права использования ПО, подписывает и возвращает Лицензиару 1 (Один) экземпляр Акта или представляет письменный мотивированный отказ от подписания Акта с указанием причин отказа и сроков их устранения, которые не могут превышать 10 (Десяти) рабочих дней со дня направления мотивированного отказа.

В случае получения от Лицензиата мотивированного отказа, Лицензиар обязуется в срок, установленный Лицензиатом, но не позднее 10 (Десяти) рабочих дней со дня направления им мотивированного отказа, устранить указанные недостатки без дополнительной оплаты со стороны Лицензиата.

Последующее подписание Акта Лицензиатом выполняется в предусмотренном настоящим разделом ТЗ порядке в срок не позднее 10 (Десяти) рабочих дней с даты предоставления Акта повторно.

6.2. Оплата предоставленного права использования ПО осуществляется не позднее 10 (Десяти) рабочих дней с даты подписания Сторонами Акта.

6.3. Договор подлежит казначейскому сопровождению в соответствии с пунктом 7 части 2 статьи 5 Федерального закона от 30 ноября 2024 г. № 419-ФЗ «О федеральном бюджете на 2025 год и на плановый период 2026 и 2027 годов».

Приложение 2
Рекомендуемая форма предоставления коммерческого предложения

На бланке организации (при наличии)

№__от ____ 20 _ г.

на № ___ от ____

АНО «Цифровой аудит»

КОММЕРЧЕСКОЕ ПРЕДЛОЖЕНИЕ

В ответ на запрос от _____ № ___ _____ *(наименование организации, ИНН)* сообщает ценовую информацию на _____ (*указать предмет закупки*) согласно условиям, указанным в запросе и Техническом задании:

№ п/п	Наименование приобретаемой продукции	Объем закупаемой продукции (количество лицензий (тип лицензии при наличии), шт.)	Цена за единицу, *с НДС / НДС не облагается*[1], руб.	Общая стоимость, *с НДС / НДС не облагается*[2], руб.
1	Программное обеспечение платформы управления контейнеризацией _____ *(указывается наименование предлагаемого ПО)*			

Итого стоимость _____ *(указать предмет закупки)* на условиях, указанных в запросе, составляет _____ **(_____) рублей ___ коп.,** ***включая НДС _% / НДС не облагается на основании _____.***

Стоимость включает в себя все затраты, издержки и иные расходы исполнителя, необходимые для осуществления им своих обязательств в полном объеме и надлежащего качества, в том числе все налоги, пошлины, сборы и другие обязательные платежи, взимаемые на территории Российской Федерации.

Срок действия предлагаемой цены составляет:_____*(рекомендуется указывать срок не менее 60 календарных дней).*

Настоящим подтверждаем, что предлагаемое к закупке ПО соответствует условиям Технического задания, указанного в запросе АНО «Цифровой аудит» от ____ № _____ *(при необходимости приложить соответствующие подтверждающие документы, ссылки, реквизиты документа и пр).*

Представитель организации ФИО м.п. (при наличии)

[1] Необходимо выбрать один из вариантов.
[2] Необходимо выбрать один из вариантов.