**Наименование закупки:** Приобретение программного или аппаратного средства класса «сканер уязвимостей».

**Лот № 1:** Приобретение программного или аппаратного средства класса «сканер уязвимостей».

**Срок выполнения работ:** Срок поставки не более 10 дней.

**Срок действия конкурсной заявки:** 30 дней.

**Планируемая сумма закупки:** 2 576 100,0 сом.

**ГОКЗ** – Декларация.

**Оплата будет производиться в течении 5 рабочих дней с момента выставления счета на оплату.**

# **Технические требования для сканера уязвимостей**

| **№ раздела** | **Раздел** | **Требования** | **Обязательное/ Желательное** | **Ответ Участника конкурса на поставку ПО** |
| --- | --- | --- | --- | --- |
| **1** | **Лицензирование** | Решение должно включать лицензию, позволяющую сканировать активы на наличие уязвимостей в количестве 500 IP адресов. | Обязательное |  |
| **2** | **Непрерывный мониторинг активов и их уязвимостей** | Система должна включать в себя встроенную возможность активного и пассивного (для обнаружения активов) сканирования для полной видимости уязвимостей и соответствия стандартам. | Обязательное |  |
| Система должна обеспечивать сканирование без агентов и на основе агентов. | Обязательное |  |
| **3** | **Архитектура** | Все компоненты системы должны устанавливаться локально и не нуждаться в подключении к сети интернет. | Обязательное |  |
| Система должна иметь центральную консоль для всех своих компонентов, которая развертывается локально, чтобы собирать, управлять и анализировать информацию об уязвимостях, не отправляя её в облако. | Обязательное |  |
| Система должна иметь возможность локально устанавливать активные сканеры в сети и подключать их к центральной консоли. | Обязательное |  |
| Система должна иметь возможность локально устанавливать агенты на конечные точки и подключать их к центральной консоли. | Обязательное |  |
| Система должна иметь возможность локально устанавливать пассивные сканеры и подключать к центральной консоли. | Обязательное |  |
| Система должна централизовать и полностью автоматизировать ежедневное обновление базы уязвимостей. | Обязательное |  |
| Система должна поддерживать возможность обновления (включая обновления базы уязвимостей и самого программного обеспечения) в автономном режиме, без использования подключения к сети Интернет (офлайн-обновления). | Обязательное |  |
| Система должна обеспечивать хранение данных, которое не зависит от стороннего продукта, предоставляющего базу данных. | Обязательное |  |
| Система должна иметь комплексный, открытый REST API для автоматического создания сценариев сканирования и экспорта данных по безопасности. | Обязательное |  |
| Обеспечение регистрации всех выполняемых операций с возможностью передачи логов в централизованную систему хранения | Обязательное |  |
| **4** | **Контроль доступа** | Система должна обеспечивать управление доступом на основе ролей, чтобы контролировать доступ пользователей к определенным наборам данных и функциям, доступных этим пользователям. | Обязательное |  |
| Система должна позволять администраторам определять роли в зависимости от должностных обязанностей и соответствующих уровней доступа к функциям. | Желательное |  |
| Система должна иметь возможность интеграции с LDAP для проверки подлинности пользователя. Система должна поддерживать несколько серверов LDAP для аутентификации. | Желательное |  |
| Система должна иметь подробный отчет об активности пользователей. | Желательное |  |
| Система должна позволять администраторам ограничивать доступ для отдельных пользователей или групп к определенным спискам активов, политикам сканирования и репозиториям уязвимостей. | Желательное |  |
| Система должна разрешать администраторам назначать ресурсы для каждого пользователя или группы, например, политики сканирования, списки активов, запросы и учетные данные. | Желательное |  |
| Система должна позволять администраторам ограничивать разрешение на проведение: полного сканирования, сканирования с использованием определенных политик. | Обязательное |  |
| В системе должна быть предусмотрена возможность планирования времени, чтобы предотвратить сканирование в запрещенные часы. | Обязательное |  |
| Система должна обеспечивать возможность принятия и изменения риска уязвимостей. | Желательное |  |
| **5** | **Сканирование** | Система должна поддерживать разные платформы для размещения сканера, включая операционные системы Windows, Linux, macOS, а также виртуальные и аппаратные устройства. | Обязательное |  |
| Система должна поддерживать различные платформы для размещения агента, включая операционные системы Windows, Linux, macOS | Обязательное |  |
| Система должна предоставлять пользователям возможность развертывать дополнительные сканеры в своей среде | Обязательное |  |
| Система должна предоставлять пользователям возможность развертывать дополнительные агенты в своей среде | Обязательное |  |
| Система должна предоставлять пользователям возможность развертывать дополнительные пассивные сканеры в своей среде | Обязательное |  |
| Система должна обеспечивать возможность настройки портов, протоколов и служб для подключений к сканерам, развернутым по всей сети ИТ-инфраструктуры. | Обязательное |  |
| Система должна настраиваться, чтобы регулировать сканирование для предотвращения генерации трафика, достаточного для нарушения нормальной работы сетевой инфраструктуры. | Обязательное |  |
| Система должна обеспечивать возможность поддержания автономного сканирования и импорта результатов на сервер. | Желательное |  |
| Система должна позволять ввод и безопасное хранение учетных данных пользователей, включая локальные и доменные учетные записи Windows, а также su и sudo для Unix систем с доступом по «ssh». | Обязательное |  |
| Система должна обеспечивать возможность повышения привилегий от обычных пользователей к администратору. | Желательное |  |
| Система должна поддерживать неограниченное количество учетных данных «ssh». | Желательное |  |
| **6** | **Активы** | Система должна поддерживать возможность обнаружения активов, не использующих лицензию. | Обязательное |  |
| Система должна обеспечивать возможность активного сканирования и пассивного мониторинга сети для обнаружения активов. | Обязательное |  |
| Система не должна полагаться на сторонние сканеры для обнаружения активов, сканирования портов или идентификации ОС. | Желательное |  |
| Система должна обеспечивать обнаружение веб-служб и служб баз данных. | Обязательное |  |
| Система должна уметь обнаруживать службы, работающие на нестандартных портах. | Обязательное |  |
| Система должна уметь выявлять службы, в которых не отображаются баннеры подключения. | Обязательное |  |
| Система должна быть способна тестировать несколько экземпляров одной и той же службы, работающей на разных портах. | Обязательное |  |
| Система должна уметь сканировать "мертвые" конечные точки (устройства, не отвечающие на ICMP запросы). | Обязательное |  |
| Система должна поддерживать использование SMB и WMI для сканирования систем Windows. | Обязательное |  |
| Сканер должен поддерживать безопасное соединение (ssh) с возможностью повышения привилегий для сканирования уязвимостей и аудита конфигурации в системах Unix. | Обязательное |  |
| Система должна иметь возможность собирать/импортировать и отображать данные об активах IT, сетей в единой консоли. | Желательное |  |
| Система должна обеспечить возможность настройки политик сканирования для минимального воздействия на сети и цели сканирования***.*** | Обязательное |  |
| Система должна обеспечивать обнаружение точек беспроводного доступа (WAP) посредством активного и пассивного сканирования. | Обязательное |  |
| Система должна обеспечивать возможность обнаружения новых устройств и отправки предупреждений посредством электронной почты, системного журнала или консольных сообщений. | Обязательное |  |
| Система должна обеспечивать возможность автоматического запуска сканирования новых устройств. | Обязательное |  |
| **7** | **Сценарии/шаблоны сканирования** | Система должна поддерживать сканирование с аутентификацией и без аутентификации для локального и удаленного обнаружения уязвимостей без необходимости установки агента на стороне клиента на целевом устройстве. | Обязательное |  |
| Система не должна полагаться на сторонние сканеры для сканирования уязвимостей. | Желательное |  |
| Система должна уметь отслеживать изменения DHCP, связывая результаты сканирования с именами устройств в системе. | Обязательное |  |
| Система должна поддерживать возможность сохранения результатов сканирования неактивных конечных станций в течение настроенного периода времени. | Обязательное |  |
| Система должна включать подробные данные о результатах сканирования, включая такую информацию, как найденные версии DLL. | Обязательное |  |
| Система должна сообщать об известных недостатках в заданной цели, используя базы данных уязвимостей, такие как CVE, OSVDB, Bugtraq (BID) или их сочетание. | Обязательное |  |
| Система должна поддерживать сканирование уязвимостей на соответствие PCI. Система должна включать предопределённые профили сканирования PCI, отвечающие текущим критериям PCI DSS для сканирования сети | Обязательное |  |
| Система должна обеспечивать сбор, мониторинг и аудит статуса установленных исправлений (патчей) для операционных систем и приложений Microsoft, таких как Windows 10, 11 и все последующие версии, Windows Server 2016, Windows Server 2019 и все последующие версии, Internet Explorer, Microsoft Edge, Microsoft Office, IIS, Exchange и другие. | Обязательное |  |
| Система должна обеспечивать аудит исправлений для всех основных операционных систем Unix, включая macOS, Linux и другие. | Обязательное |  |
| Система должна обеспечивать аудит поправок для сетевой инфраструктуры, включая Cisco, Check Point и другие. | Обязательное |  |
| Система должна уметь собирать/импортировать и отображать данные об уязвимости ИТ сетей для единой визуализации уязвимостей в объединенных сетях ИТ. | Желательное |  |
| Система должна предоставлять отчеты об угрозах, выявленных вредоносных программ и бот-сетей. | Обязательное |  |
| Система должна обеспечивать приоритизацию уязвимостей с использованием аналитики угроз в реальном времени и алгоритмов для оценки уязвимостей | Обязательное |  |
| Система должна обеспечивать приоритизацию уязвимостей, помогающую пользователям понять ключевые факторы, влияющие на каждую оценку уязвимости | Желательное |  |
| Система должна включать оценку уязвимости в соответствии с общей системой оценки уязвимостей (CVSS). | Обязательное |  |
| Система должна обеспечивать настраиваемый механизм оценки уязвимостей, основанный на принятых в отрасли стандартах, таких как CVSS. | Желательное |  |
| Система должна предоставлять информацию об использовании вредоносных программ на конечном устройстве. | Обязательное |  |
| Система должна отслеживать жизненный цикл уязвимостей по отношению к отдельным конечным устройствам, а также средам, включая дату первого обнаружения, последнего наблюдения и устранения уязвимости. | Обязательное |  |
| Система должна поддерживать сканирование серверов VMware на уязвимости. | Обязательное |  |
| Система должна позволять сканировать устройства по расписанию. | Обязательное |  |
| Система должна позволять включать или отключать проверки на определенные уязвимости при сканировании. | Обязательное |  |
| Система должна автоматически запускать и останавливать сканирование по расписанию без вмешательства пользователя. | Обязательное |  |
| Система должна разрешать прекращать и возобновлять сканирование вручную. | Обязательное |  |
| Система должна позволять запускать сканирование, незавершенное в установленные сроки, или переносить на следующий запланированный период. | Желательное |  |
| Система должна иметь возможность принимать цели сканирования в разных форматах, включая имена DNS, диапазоны IP-адресов и классы IP, а также предварительно определенные списки активов. Также должен поддерживаться импорт списка IP-адресов, содержащихся в файле. | Обязательное |  |
| Система должна поддерживать сканирование IPv6 с пассивным обнаружением активов IPv6. | Обязательное |  |
| Система должна обеспечивать возможность отключения сканирования периферийных устройств, например, принтеров и др.. | Желательное |  |
| **8** | **Агент** | Агент должен собирать и отправлять данные на центральную консоль. | Обязательное |  |
| Агенты должны быть подключены и управляться через локальную консоль. | Обязательное |  |
| Агент должен предоставлять возможность регулировать свою нагрузку на конечную точку, для предотвращения нарушения рабочих процессов. | Обязательное |  |
| Агент должен иметь возможность соединяться с консолью через прокси-сервер. | Обязательное |  |
| Система должна иметь возможность создавать группы агентов для автоматизации процесса обнаружения уязвимостей. | Желательное |  |
| Система должна предоставлять информацию о статусе агентов. | Обязательное |  |
| Агент должен иметь уникальный идентификатор для обнаружения одного и того же устройства в разных подсетях. | Обязательное |  |
| **9** | **Пассивное сканирование** | Пассивный сканер должен включать в себя возможность сканирования уязвимостей путем мониторинга сетевого трафика без активного сканирования. | Обязательное |  |
| Пассивный сканер должен отображать обнаруженные в трафике уязвимости в реальном времени. | Обязательное |  |
| Пассивный сканер должен поставляться тем же вендором, что и основная система. | Желательное |  |
| Пассивный сканер должен предоставлять информацию об отдельной сети, сетях в целом или любой конкретной группе хостов. | Обязательное |  |
| **10** | **Аудит на соответствие** | Система должна поддерживать аудит на соответствие как с аутентификацией, так и без аутентификации, с или без необходимости установки агента на стороне клиента на конечной точке. | Обязательное |  |
| Система не должна полагаться на сторонние сканеры для аудита/оценки конфигурации безопасности. | Желательное |  |
| Система должна предоставлять единое представление обо всех результатах аудита уязвимостей и соответствия требованиям. | Желательное |  |
| Система должна обеспечить аудит конфигураций для соответствия нормативным требованиям и другим отраслевым стандартам, и стандартам лучшей практики поставщиков. | Желательное |  |
| Система должна обеспечивать аудит конфигурации, основанный на лучших практиках для таких поставщиков, как Microsoft, Cisco и VMware. | Желательное |  |
| Система должна обеспечить аудит операционных систем Microsoft для проверки параметров безопасности и конфигураций. | Желательное |  |
| Система должна обеспечить аудит всех основных операционных систем Unix для проверки параметров безопасности и конфигураций. | Желательное |  |
| Система должна обеспечивать аудит баз данных для проверки параметров безопасности и конфигураций таких как: PostgreSQL, Microsoft SQL, Oracle, MySQL и т.д. | Желательное |  |
| Система должна обеспечивать аудит приложений для проверки параметров безопасности и конфигураций таких как: Internet Explorer, Microsoft Edge, Google Chrome, Microsoft Office и т.д. | Желательное |  |
| Система должна обеспечивать аудит сетевой инфраструктуры для проверки параметров безопасности и конфигураций таких как: Cisco, HP, F5 и т.д. | Желательное |  |
| Система должна обеспечивать аудит определенных продуктов безопасности конечных точек на предмет статуса установки и обновления. | Обязательное |  |
| Система должна позволять настраивать политики аудита в соответствии с потребностями организации. | Желательное |  |
| **11** | **Автоматизация** | Система должна обеспечивать полную автоматизацию сканирования, создания отчетов и предупреждений*.* | Обязательное |  |
| Система должна иметь отдельные панели для отображения уязвимостей обнаруженных: активно, пассивно, сканирования на соответствие. | Желательное |  |
| Система должна объединять результаты отдельных сканирований уязвимостей с возможностью фильтрации, чтобы обеспечить возможность детализации и анализа. | Желательное |  |
| Система должна иметь отдельные представления активных и устраненных уязвимостей с автоматическим переносом уязвимостей из активных на устраненные после того, как сканирование определяет, что уязвимости больше нет. | Обязательное |  |
| Система должна иметь возможность отмечать уязвимость как ранее устраненную, но появившуюся снова | Желательное |  |
| Система должна обеспечивать комплексную фильтрацию обнаруженных уязвимостей с возможностью детализации по следующим параметрам, но не ограничиваться ими: IP адрес, идентификатор агента, актив, аудит файл, идентификатор CVE, оценка CVSS v2, оценка CVSS v3, Имя DNS, доступность эксплойта, порт, протокол, уровень критичности, дата первого обнаружения, дата последнего обнаружения, текст уязвимости. | Обязательное |  |
| В системе должна быть возможность добавлять теги к активам, политикам, учетным данным или запросам с настроенным описанием для улучшения фильтрации и управления объектами. | Желательное |  |
| Система должна иметь панель для аналитика безопасности, которая автоматически устанавливает приоритеты и оптимизирует решения для исправления уязвимостей | Желательное |  |
| Система должна позволять исключать из сканирования заданные IP-адреса на  определенный промежуток времени. | Обязательное |  |
| Система должна обеспечивать функцию создания задач и возможность интеграции со сторонними системами для отслеживания задач. | Желательное |  |
| Система должна поддерживать назначение задач отдельным пользователям. | Желательное |  |
| Система должна обеспечивать возможность уведомления об уязвимости и событии. | Обязательное |  |
| Система должна поддерживать создание уведомлений на основе результатов сканирования уязвимостей или аудита конфигурации. | Обязательное |  |
| Уведомление должно включать: настраиваемое электронное письмо с несколькими переменными контекста, создание задач, запуск сканирования, создание события в системном журнале, создание отчета и сообщения пользователей. | Желательное |  |
| **12** | **Составление отчетов** | Система должна поддерживать создание отчетов, настраиваемых с использованием шаблонов, предоставленных вендором или без шаблонов. | Обязательное |  |
| Система должна предоставлять встроенные отчеты по сканированию и журналы системы. | Обязательное |  |
| Система должна обеспечивать возможность полной автоматизации отчетов, включая выполнение и отправку по расписанию, а также отправку отчетов после сканирования. | Желательное |  |
| Система должна обеспечивать возможность просмотра результатов в консоли независимо от процесса создания отчетов. | Обязательное |  |
| Система должна поддерживать возможность создания отчетов в следующих форматах: PDF, CSV, MS Excel | Обязательное |  |
| Система должна предоставлять отчеты высокого уровня относительно показателей безопасности и соответствия стандартам. | Желательное |  |
| **13** | **Информационные панели** | Система должна включать в настройку графические панели и созданные шаблоны панелей для отображения уязвимостей и состояния безопасности. | Обязательное |  |
| Система должна обеспечивать настройку результатов сканирования на информационных панелях с использованием отфильтрованных результатов для определения нескольких линий метрик на одном графике. | Желательное |  |
| Система должна позволять каждому пользователю создавать несколько пользовательских информационных панелей. | Желательное |  |
| Система должна давать пользователям возможность совместно использовать информационные панели. | Обязательное |  |
| Система должна поддерживать настройку параметров шаблона и форматирование информационных панелей. | Желательное |  |
| **14** | **Сканирование ресурсов, доступных из сети Интернет** | Система должна обеспечивать выявление активов и сервисов организации, имеющих доступ из сети Интернет и потенциально доступных для несанкционированного доступа со стороны злоумышленников, без применения активного сканирования | Обязательное |  |
| Система должна собирать и отображать основные сведения об обнаруженных активах:   * имя хоста (домен или поддомен), * IP-адрес, * открытые сетевые порты. | Обязательное |  |
| Информация о внешних ресурсах организации должна обновляться не реже одного раза в квартал, чтобы поддерживать актуальность. | Желательное |  |

**Квалификационные и иные требования:**

1. Предоставить сведения о наличии выполнения не менее 2-х аналогичных договоров/услуг за последние 2 года;
2. Поставщик должен являться официальным партнером или дистрибьютером компании (предоставить MAF);
3. Предоставить сканированную копию оригинала свидетельства о регистрации;
4. Предоставить сканированную копию оригинала устава;
5. Предоставить письменное подтверждение об отсутствии аффилированности, а также информацию об их бенефициарных владельцах;
6. Предоставить справку с Государственной Налоговой Службы при Министерстве финансов Кыргызской Республики об отсутствии задолженности по налогам и страховым взносам (в случае если поставщик является резидентом Кыргызской Республики);
7. Предоставить заполненную конкурсную заявку и декларацию (подписанный представителем подрядной организации имеющие все полномочия и утвержденной печатью организации) согласно приложению № 1 и 2;
8. Предоставить коммерческое предложение и заполненное техническое задание по лоту, по которому подается заявка, включая все налоги и сборы, предусмотренные законодательством КР.

**Компания может отклонить конкурсную заявку в случаях, если:**

1. Участник, представивший данную конкурсную заявку, не соответствует квалификационным требованиям, установленным в конкурсной документации;
2. Участник не подписал декларацию, гарантирующую предложение, либо не представили ГОКЗ (если требуется условием конкурсной документации);
3. Участник имеет задолженность по налогам или по страховым взносам по государственному социальному страхованию и социальным выплатам;
4. Технические параметры, предложенные в конкурсной заявке, не соответствуют технической спецификации конкурсной документации;
5. Данная конкурсная заявка, по существу, не отвечает требованиям конкурсной документации;
6. Имеется соответствующее заключение Комплаенс-офицера о неблагонадежности участника.

**Приложение № 1. Конкурсная заявка**

**Конкурсная заявка**

Номер объявления:

Кому: ЗАО «Межбанковский Процессинговый Центр»

Наименование конкурса: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Изучив опубликованную на сайте www.tenders.kg/www.ipc.kg конкурсную документацию, мы нижеподписавшиеся:

\_\_\_\_\_\_\_\_\_\_\_\_(Наименование, ИНН) в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

предлагаем поставить \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в соответствии со всеми условиями и требованиями конкурсной документации, подтверждаемые заполненной таблицей цен, которая является частью настоящей конкурсной заявки.

Мы, включая всех членов простого товарищества и субпоставщиков в отношении любой части договора в соответствии с настоящей конкурсной документацией подтверждаем свою правомочность к участию в данном конкурсе согласно заполненным условиям правомочности участника.

Мы обязуемся, в случае определения нашей конкурсной заявки победившей, которая была сформирована и подана на адрес электронной почту \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1) Предоставить все оригиналы документов, входящие в состав конкурсной заявки;

2) Поставить товар в соответствии со сроками, приведенными в конкурсной документации. До подготовки и оформления официального договора данная конкурсная заявка вместе с Вашим письменным подтверждением ее принятия и Вашим уведомлением о присуждении договора будет выполнять роль обязательного договора между нами.

Мы понимаем, что Вы не обязаны принять конкурсную заявку с наименьшей оцененной стоимостью или вообще какую-либо из заявок, полученных Вами.

Имеющий все полномочия подписать конкурсную заявку от имени \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Должность, подпись

М.П.

**Приложение № 2. Декларация, гарантирующая предложение поставщика**

**Декларация, гарантирующая предложение поставщика**

Номер конкурса: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Название конкурса: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Участник конкурса: *наименование, ИНН\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

Закупающая организация: ЗАО «Межбанковский Процессинговый Центр»

Принимая во внимание, что мы, представили свое предложение в рамках вышеуказанного Конкурса, на закупку \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (далее именуемую «Предложение поставщика»).

Настоящим доводится до всеобщего сведения, что Участник конкурса принял на себя следующие обязательства перед Закупающей организацией:

1. Участник конкурса не отзовет и не изменит свое настоящее предложение после ее вскрытия и до истечения срока ее действия, указанного Участником конкурса в Предложении поставщика;
2. Участник конкурса подпишет Договор в соответствии с предложением, в случае если будет определен победителем Конкурса;
3. Участник конкурса предоставит Гарантийное обеспечение исполнения Договора в соответствии с конкурсной документацией, если требуется условиями Конкурса;

Настоящим подтверждается, что при невыполнении любого из указанных обязательств, Закупающая организация инициирует включение Участника конкурса в «Базу данных ненадежных (недобросовестных) поставщиков (подрядчиков)».

Настоящая декларация остается в силе до истечения срока действия предложения.

Руководитель организации

либо лицо, имеющее полномочия ФИО

М.П.