**Техническое задание**

**Наименование закупки:** Приобретение системы Privileged Access Management.

**Лот № 1:** Приобретение системы Privileged Access Management.

**Срок выполнения работ:** Срок поставки 10 дней со дня подписания Договора.

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

**ГОКЗ** – Декларация.

|  |  |  |  |
| --- | --- | --- | --- |
| **Предмет закупки** | **Количество** | **Технические характеристики** | **Иные требования** |
|  |  | - Поддержка многофакторной аутентификации (MFA) для привилегированных пользователей |  |
| Решение для управления привилегированным доступом PAM | 70 пользовательских лицензий | Управление паролями и ротация паролей  Уведомления и оповещения  Отчеты и информационные панели - Аудит и мониторинг сессий | Поставка лицензии, настройка, обучение персонала |
| - Централизованное управление доступом |
|  |  | - Возможности интеграции с текущей ИТ-инфраструктурой и системами безопасности (например, AD, SIEM и т.д.) |  |

**Техническое задание на решение по управлению привилегированными учетными записями (PAM)**

1. ТЕХНИЧЕСКАЯ КВАЛИФИКАЦИЯ

1.1. Участник тендера должен представить доказательство, выданное производителем Решения для этого Технического задания, информирующее о том, что Подрядчик может и уполномочен продавать продукты и услуги, являющиеся предметом Соглашения.

1.2. ВИРТУАЛЬНАЯ МАШИНА

1.2.1. Решение должно быть доступно для приобретения в виде виртуального устройства (VA - virtual appliance);

1.2.2. Решение должно иметь важные встроенные программные компоненты, интегрированные в само решение без необходимости использования внешних ресурсов:

1.2.2.1. Оптимизированная и усиленная по всем аспектам (приложение, база данных, файловая система и т. д.) операционная система на базе Linux на базе одного виртуального устройства на VMWare, ProxMox, Nutanix, Hyper-v, Openstack. В системе должен работать только минимальный набор служб, подчиняющихся принципу минимальных привилегий, и ядро, адаптированное к функциональности решения.

1.2.2.2. Собственная база данных, где лицензия не требуется.

1.2.2.3. Собственный интегрированный веб-сервер.

1.2.2.4. Встроенный веб-интерфейс, никаких лицензий и дополнительных серверов не требуется.

1.2.2.5. Все вышеперечисленные компоненты должны быть реализованы на базе единого виртуального устройства.

1.3. Решение должно работать как шлюз для RDP и SSH Proxy, то есть администратор может напрямую использовать адрес PAM системы в RDP и SSH клиентах для доступа к целевым системам без использования RDS сервера или веб-доступа через браузер.

1.4. Решение должно иметь прозрачную аутентификацию в целевой системе или на сетевом устройстве. Решение должно инициировать сеанс, напрямую вводя учетные данные на экране входа в систему и выступая в качестве прокси для сеанса между пользователем и целевой системой, чтобы пароль не был доступен инициатору запроса доступа;

1.5. Решение должно удалять учетные данные, встроенные в исходный код, сценарии и файлы конфигурации, делая пароли управляемыми и невидимыми для разработчиков и персонала ИТ-поддержки;

2. ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

2.1. Архитектура системы

2.1.1. Решение должно обеспечивать одновременное подключение не менее X привилегированных пользователей без ограничений по количеству целевых систем, к которым идет подключение;

2.1.2. Лицензия на Решение должно также включать в себя права на отказоустойчивый кластер, состоящий из не менее 2 (двух) узлов;

2.1.3. Решение должно управлять всей средой без необходимости устанавливать агенты или какое-либо программное обеспечение на целевые системы или сетевые устройства;

2.1.4. Решение должно создавать видео и текстовые журналы сеансов, которые хранятся в безопасном, зашифрованном и защищенном хранилище, где контролируются любые изменения, которые ставят под угрозу целостность этих доказательств;

2.1.5. Решение должно автоматически создавать пароли повышенной сложности согласно правилам каждой технологии и Политике безопасности компании;

2.1.6. База данных должна предоставляться как неотъемлемая часть решения.

2.1.7. База данных должна находиться в «защищенной» среде, с механизмом экранирования и шифрования операционной системы и документацией, подтверждающей выполнение этих требований;

2.1.8. Должна быть возможность использования шифрования базы данных для хранения паролей учетных данных, а также должна быть совместимость хотя бы с одним из следующих методов и стандартов шифрования:

а) AES с 256-битными ключами;

в) Шифрование PKCS#11 или выше с использованием аппаратного обеспечения с использованием устройств HSM, должным образом одобренных производителем для предлагаемого решения.

2.1.9. Для операций аутентификации и согласования сеансовых ключей система должна позволять использовать алгоритмы шифрования с открытым ключом RSA длиной не менее 2048 бит.

2.1.10. Должна быть включена опция резервного копирования/восстановления всех данных и настроек решения и должна быть возможность администратору планировать резервное копирование на определенную дату и время, и экспорт резервных копий на удаленный SFTP-сервер.

2.1.11. Решение должно поддерживать сохранение всех отчетов и файлов истории, включая записи сеансов, без необходимости восстановления резервной копии в течение как минимум 90 дней.

2.1.12. Решение должно обеспечивать резервное хранение отчетов и журналов приложений в течение как минимум двух лет, а записей сеансов — как минимум один год.

2.1.13. В резервной копии главного ключа системы должна быть возможность делиться на параметризованное количество частей, для того чтобы это не позволяло визуализировать целое одним человеком, а только ту часть, которая принадлежит каждому из них.

2.1.14. Решение должно иметь функционал по обеспечению репликации в другие центры обработки данных.

2.1.15. При использовании кластера, в случае сбоя одного из серверов в локальном кластере хранилищ паролей высокой доступности каждый из серверов должен обрабатывать все запросы на доступ без каких-либо потерь в производительности или функциональности;

2.1.16. При использовании кластера, все изменения, внесенные в локальный кластер хранилищ паролей высокой доступности, должны автоматически реплицироваться на другие резервные серверы синхронно и с максимальной задержкой 50мс.

2.2. Управление

2.2.1. Решение должно иметь все функции, предоставляемые одним производителем, без зависимости сторонних инструментов или модулей;

2.2.2. Возможность связи со службами каталогов по протоколу LDAPS;

2.2.3. Решение должно иметь единый интерфейс в одном решении для управления паролями и сеансами.

2.2.4. Решение должно обеспечивать предоставление и управление всеми привилегированными учетными записями, включая учетные записи для администрирования бизнес-приложений, баз данных и сетевых устройств, а не ограничиваясь учетными записями серверной операционной системы.

2.2.5. Решение должно обеспечивать механизмы обновления безопасности:

а) автоматически;

б) по требованию.

2.2.6. Решение должно иметь возможность разрешать резервное копирование и восстановление базы данных, а также установленных конфигураций программного обеспечения со следующими возможностями:

а) Разрешать выполнение задач резервного копирования и шифрования без необходимости использования сторонних агентов, обеспечивая тем самым максимально возможный уровень безопасности и целостности копируемых данных;

б) Разрешать выполнение автоматического резервного копирования по расписанию.

2.3. Управление паролями

2.3.1. Решение должно управлять ключами SSH и сканировать серверы Linux, дополнительно идентифицировать и публиковать ключи SSH.

2.3.2. Решение должно автоматически менять пароли в запланированное время после того, как они были выпущены для использования или срок их действия, истек;

2.3.3. Решение должно периодически консолидировать пароли для выявления изменившихся паролей в управляемых системах;

2.3.4. Решение должно иметь возможность управления привилегированными паролями в приложениях и интегрироваться с устаревшими системами.

2.3.5. Решение должно освобождать или отзывать весь доступ к данным учетным данным в автоматическом и немедленном порядке;

2.3.6. Решение должно уведомлять по электронной почте или SMS о новых запросах на одобрение доступа лицам, ответственным за учетные данные;

2.3.7. Решение должно разрешать онлайн-мониторинг использования учетной записи и отключения сеанса;

2.3.8. Решение должно представлять функцию «разбить стекло» (break glass) для экстренного доступа к учетным записям, что позволит получить доступ к защищенным активам в экстренном порядке, без необходимости предварительного согласования в учетных записях, к которым пользователь не имел бы доступа, без потери отслеживаемости;

2.3.9. Решение должно предоставлять функцию Discovery для поиска новых серверов, сетевых элементов и баз данных с возможностью автоматического получения учетных записей, созданных на этих новых устройствах, включая возможность обнаружения SSL-сертификатов, используемых на управляемых устройствах;

2.3.10. Решение должно иметь возможность блокировки определенных команд с функцией прерывания сеанса, если пользователь выполнит неподходящую команду;

2.3.11. Решение должно находить конкретные команды, выполняемые пользователем через командную строку в журналах или записанных сеансах;

2.3.12. Решение должно настраивать немедленные оповещения при выполнении определенных команд привилегированными пользователями;

2.3.13. Решение должно иметь возможность формирования отчетов на основе журналов и экспорта их в файлы формата «.csv»;

2.3.14. Решение должно позволять администратору настраивать связь со сторонними приложениями с использованием скриптов, макросов, вызовов исполняемых файлов, разных языков программирования и принимать разные протоколы, включая, как минимум, RPC, WinRM, SSH, HTTP/HTTPS REST API;

2.3.15. Решение должно позволять создавать политики паролей в иерархическом порядке или по уровням безопасности, позволяя создавать дифференцированные пароли для групп активов с разных платформ или критичности.

2.3.16. Решение должно иметь механизм экспорта файла с последними паролями в удаленный репозиторий в зашифрованном виде и защищенным паролем двойного хранения для восстановления пароля в случае полного сбоя решения;

2.3.17. Решение должно иметь возможность управлять учетными данными, которые находятся в системах, расположенных в нескольких географических местоположениях или в разных доменах;

2.3.18. Решение должно иметь возможность управлять паролями привилегированных приложений, чтобы избежать использования паролей, встроенных в исходный код.

2.3.19. Решение не должно зависеть от установки агентов для смены паролей.

2.4. Ротация паролей

2.4.1. Решение должно предоставлять функционал автоматической смены паролей для серверов (Unix, Linux, Windows), баз данных (MS SQL, ORACLE, MYSQL, PostgreSQL), веб-приложений, сетевых устройств, мейнфреймов;

2.4.2. Решение должно иметь гибкость настройки надежности сгенерированного пароля;

2.4.3. Решение должно создавать записи изменения, отчеты о мониторинге, отчеты и оповещения об ошибках и успехах;

2.4.4. Решение должно иметь возможность реконфигурации/настройки скриптов или плагина смены пароля для настройки случаев, требующих определенных параметров для ротации паролей;

2.4.5. Решение должно иметь возможность делать шаблоны смены паролей доступными, чтобы их можно было открывать, редактировать и проверять;

2.4.6. Решение должно изменять пароли в HTTP/HTTPS-приложениях с помощью шаблонов.

2.5. Контроль доступа

2.5.1. Решение должно позволять контролировать выполнение критических команд как минимум по «белому списку» и «черному списку».

2.5.2. Решение должно иметь время окончания сеанса, настраиваемое системным администратором.

2.5.3. Решение должно позволять параметризацию максимального количества активных сеансов на одного пользователя.

2.5.4. Решение должно поддерживать отключение сеанса из-за активности/неправильного использования предварительно зарегистрированных в системе команд.

2.5.5. Решение должно выполнять блокировку команд, прерывание сеанса и запись в журнал выполнения — на основе черного списка;

2.5.6. Решение должно выполнять мониторинг команд и запись в журнал выполнения — на основе белого списка;

2.5.7. Решение должно иметь возможность блокировки и аудита определенных команд, а также возможность поиска в журналах\записях;

2.5.8. Решение должно иметь рейтинг команд в соответствии с уровнем риска каждой команды.

2.5.9. Решение должно позволять назначать привилегии группам пользователей, связанных с одним или несколькими управляемыми объектами.

2.5.10. Решение должно обеспечивать интеграцию с инструментами управления инцидентами (ITSM) для проверки открытых заявок в процессе утверждения доступа.

2.6. Интеграция и совместимость

2.6.1. Решение должно включать с помощью сценария создание новых соединителей на основе доступа SSH и RDP, чтобы можно было поддерживать новые интерфейсы аутентификации активов;

2.6.2. Решение должно быть совместимым с операционными системами: Windows Server 2016 или выше, Red Hat Enterprise, Debian, CentOS, IBM zOS , Solaris;

2.6.3. Решение должно поддерживать приложения Windows: учетные записи служб и пулы приложений IIS;

2.6.4. Решение должно быть совместимым с базами данных: Oracle, Oracle RAC, MSSQL, MySQL, Sybase ASE и IQ, MongoDB, PostgreSQL;

2.6.5. Решение должно быть совместимым с хранилищами: Synology, Hitachi, Isilon, EMC и IBM;

2.6.6. Решение должно предоставлять SDK (комплект разработки программного обеспечения) или API (интерфейс прикладного программирования), который можно настроить так, чтобы клиентские приложения могли:

а) Запрашивать учетные данные и устройства;

б) Регистрировать и изменять учетные данные устройств;

в) Запрашивать ключи SSH;

г) Регистрировать и изменять SSH-ключи.

2.7. Потоки утверждения

2.7.1. Решение должно быть гибким в процессе одобрения доступа к привилегированным учетным записям (предварительно одобренный доступ, доступ с единым одобрением и доступ с многоуровневым одобрением).

2.7.2. Решение должно позволять утверждающему лицу изменять период доступа, запрошенный пользователем.

2.7.3. Решение должно иметь возможность сравнивать предоставленные и зарегистрированные в его базе доступы с доступами, которые фактически были выполнены к активу. После сравнения система должна отобразить обнаруженные несоответствия в отчете, например, вход в систему, выполненный в активе, но не авторизованный в решении.

2.7.4. Решение должно иметь возможность уведомлять по электронной почте о новых запросах доступа людей, ответственных за утверждение.

2.8. Уведомления и оповещения

2.8.1. Решение должно иметь возможность отправлять оповещения в SIEM о паролях, отличных от паролей хранилища.

2.8.2. Решение должно быть настроено на отправку оповещений, инициируемых системой, по крайней мере, по электронной почте и SNMP, о событиях, настроенных системным администратором.

2.9. Отчеты и информационные панели

2.9.1. Решение должно позволять модулям визуализации сеансов и генерации отчетов отображать количество найденных записей и разбиение на страницы результатов для каждого выполненного поиска.

2.9.2. Решение должно позволять создавать отчеты обо всех пользователях, зарегистрированных в приложении, и их соответствующих ролях.

2.9.3. Решение должно иметь механизмы для создания отчетов по привилегированным учетным записям, например, списков активов и их управляемых учетных записей, запросов на доступ к привилегированным учетным записям, отправленных на утверждение, утвержденных или отклоненных, а также истории использования привилегированных учетных записей.

2.9.4. Решение должно содержать подробную историю всех изменений безопасности паролей, внесенных на устройствах любым пользователем.

2.9.5. Решение должно позволять создавать отчеты PCI;

2.9.6. Решение должно позволять выгружать отчеты в формат (.csv);

2.9.7. Решение должно иметь следующие информационные панели:

a) Панель подключений;

b) Панель управления использования сеансов;

c) Панель управления станцией доступа.

d) Панель мониторинга угроз в режиме реального времени

2.9.8. Решение должно иметь возможность регистрировать каждый доступ, включая доступ через веб-приложение для запросов пароля, утверждений, проверок, изменений делегирования, отчетов и других действий. Доступ к консоли управления для настройки и составления отчетов, а также все действия по смене паролей должны регистрироваться.

2.10. Поведенческий анализ

2.10.1. Решение должно осуществлять анализ сеанса пользователя на основе записи поведения. Где входит анализ переменных исходной станции, станций назначения, учетных данных, расписаний, продолжительности сеанса;

2.10.2. Решение должно выявлять дифференцированное поведение с помощью предупреждений об отклонениях в отчетах на экране или предупреждений для SIEM/SYSLOG;

2.10.3. Решение должно осуществлять анализ сеанса пользователя с оценкой критических команд с оповещениями об аномалиях в отчетах на экране или оповещениями для SIEM/SYSLOG;

2.10.4. Решение должно иметь графические информационные панели с информацией о рисках и угрозах.

2.11. Аутентификация

2.11.1. Решение должно обеспечивать встроенную многофакторную аутентификацию пользователей (MFA) с помощью одноразового пароля (OTP).

2.11.2. MFA должен также используется и для RDP/SSH сессий напрямую через PAM без использования веб-браузера и веб-консоли.

2.11.3. Решение должно быть интегрировано в базу пользователей с административными привилегиями Microsoft Active Directory, TACACS и RADIUS для предоставления доступа к платформе, а также назначения профилей доступа к функциям системы.

2.11.4. Решение должно иметь централизованную интегрированную аутентификацию через SAML и OpenID;

2.12. Управление пользователями и профилями

2.12.1. Решение должно иметь возможность разделять функции по профилям доступа.

2.12.2. Решение должно иметь гибкость создания любых новых профилей с различными комбинациями окон и функций в соответствии с потребностями бизнеса без вмешательства поставщика.

2.12.3. Решение должно иметь возможность создавать пользовательские теги для определения устройств и учетных данных;

2.12.4. Решение должно иметь возможность управлять группами и профилями доступа, интегрированными с группами AD/LDAP.

2.13. Управление и запись сеансов

2.13.1. Решение должно позволять управлять и контролировать сеансы, установленные по протоколам: HTTP, HTTPS, SSH и RDP, либо через прокси-сервер, либо через Jump сервер.

2.13.2. Видеозапись сессий должна осуществляться через веб-прокси или прозрачный прокси в оптимизированном формате;

2.13.3. Должна осуществляться запись команд, вводимых в средах RDP и SSH;

2.13.4. Решение должно иметь возможность просмотра видео сеанса, проводимого прямо в решении, без необходимости конвертировать его в видеоформат или скачивать;

2.13.5. Решение должно сжимать записанные видео. Кроме того, должны учитываться периоды неактивности сеанса.

2.13.6. Решение должно иметь возможность экспортировать записи сессий в видеоформат MP4;

2.13.7. Решение должно записывать все выполненные действия и предоставлять данные аудита пользователям с соответствующим профилем, например, профилем аудитора.

2.13.8. Решение должно хранить в журналах как минимум следующую информацию:

2.13.8.1. Идентификацию пользователя, осуществившего определенный доступ к устройству;

2.13.8.2. Идентификацию того, кто разрешил доступ пользователю;

2.13.8.3. Дату и время осуществления доступа и действий, совершенных пользователем на удаленном устройстве.

2.13.9. Механизм записи должен быть предусмотрен и развит как неотъемлемая часть решения, при этом программы от производителей, отличных от разработчика предлагаемого решения, приниматься не будут.

2.13.10. Решение должно контролировать доступ к записанным сеансам как в виде разрешения, так и путем регистрации лиц, имеющих доступ.

2.13.11. Решение должно поддерживать поиск выполненных команд и связывать эти команды с записанными и сохраненными кадрами сеанса.

2.13.12. Срок действия и очистка записей автоматически или вручную.

2.13.13. Возможность хранения и экспорта записей за пределы PAM (локальная сеть).

2.14. Автоматизация привилегированных задач

2.14.1. Решение должно выполнять задачи с помощью предварительно зарегистрированных сценариев, при этом для одного сценария может быть предоставлена возможность выбрать несколько устройств.

2.14.2. Должна быть предусмотрена возможность регистрации переменной для замены учетных данных в сценарии выполнения, чтобы не раскрывать учетные данные, которые будут использоваться при выполнении.

2.14.3. Решение должно иметь процесс согласования выполнения задач, в том числе многоуровневое согласование не менее чем с 3 уровнями.

2.14.4. Решение должно иметь отчеты с историей выполнения, с указанием, какой скрипт выполнялся, на каких устройствах, была ли ошибка и кто был инициатором запроса.

3. УСЛУГИ ПО УСТАНОВКЕ И НАСТРОЙКЕ

3.1. ПОДРЯДЧИК должен выполнить установку приобретенного решения в течение до тридцати (30) дней после получения решения;

3.2. Должна быть выполнена первоначальная конфигурация, где будет настроен IP системы для генерации и активации лицензии и дальнейшего обеспечения выполнения услуг по настройке функций, требуемых в настоящем Техническом задании;

3.3. Для завершения этапа установки и начала этапа настройки ПОДРЯДЧИК должен предоставить следующие документы:

3.3.1. План конфигурации:

3.3.1.1. Схема взаимосвязи решения;

3.3.1.2. Логическое проектирование конфигурации;

3.3.1.3. Конфигурация решения;

3.3.2. План выполнения:

3.3.2.1. График мероприятий;

4. УСЛУГА ПО ЛИЦЕНЗИРОВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

4.1. Лицензия должна быть выдана на бессрочное использование, то есть по истечении 12 (двенадцати) месяцев обновления и гарантии продукты будут продолжать использоваться контрагентом, независимо от того, приобретаются ли пакеты обновлений и техническая поддержка для последующего использования.

**Квалификационные и иные требования:**

1. Предоставить сканированную копию оригинала свидетельства о регистрации;
2. Предоставить сканированную копию оригинала устава;
3. Предоставить письменное подтверждение об отсутствии аффилированности, а также информацию об их бенефициарных владельцах;
4. 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);
5. Предоставить заполненную конкурсную заявку и декларацию (подписанный представителем подрядной организации имеющие все полномочия и утвержденной печатью организации) согласно приложению № 1 и 2;
6. Предоставить сведения о наличии выполнения не менее 2-х аналогичных договоров/услуг;
7. 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.