**Техническое задание**

Закупка производится в соответствии с требованиями Положения о закупке товаров работ, услуг для нужд частных учреждений здравоохранения ОАО «РЖД», утвержденного приказом Центральной дирекции здравоохранения от 5 марта 2021г. № ЦДЗ-18 раздел 68, размещенного на сайте заказчика: https://ufa.rzd-medicine.ru в разделе - Закупки.

 Оказание услуг по предоставлению неисключительных прав на использование средств защиты информации, установке и настройке средства защиты информации и аттестация информационной системы для подключения к Республиканской медицинской информационно-аналитической системе Республики Башкортостан

1. Срок оказания услуг: 45 (сорок пять) рабочих дней с момента подписания договора.
2. **сновные требования к оказываемым услугам:**

Услуги, по своим характеристикам соответствуют параметрам, приводимых в требованиях, перечисленных ниже:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование** | **К-во****(шт.)** | **Требования к функциональным, качественным, эксплуатационным характеристикам объекта закупки**  | **Ед. измерения** | **Наличие характеристики** |
| Сертификат активации сервиса совместной технической поддержки ПАК ViPNetCoordinator HW1000 на срок 1 год, уровень – Расширенный\* | **1** | Сертификат активации сервиса совместной технической поддержки ПАК ViPNetCoordinator HW1000 4.x, уровень - Расширенный Начало действия сертификата  |  | Наличие |
| Сертификат действует на количество имеющихся в сети ViPNet ПАК ViPNetCoordinator HW1000 4.x | Шт. | Не менее 2 |
| Срок действия сертификата активации сервиса совместной технической поддержки ПАК ViPNetCoordinator HW1000 4.x, уровень - Расширенный | мес. | Не менее 12 |
| Передача права на использование версии 4.x программного обеспечения ПАК ViPNetCoordinator HW1000 4.x\* | 2 | Передача права на использование версии 4.x программного обеспечения ПАК ViPNetCoordinator HW1000 4.x |  | Наличие |
| Дистрибутив с ПО ViPNetCoordinator HW1000  | Шт. | Не менее 2 |
| Исполнитель обязан обновить ПАК ViPNetCoordinatorHW до новой версии  |  | Наличие |
| Средство защиты информации от несанкционированного доступа - срок действия лицензии -1 год[[1]](#footnote-2) | **2** | ***СЗИ должно осуществлять:**** защиту серверов и рабочих станций от НСД;
* контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты;
* разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации;
* разграничение доступа пользователей к информации;
* контроль утечек информации;
* регистрацию событий безопасности и аудит;
* паспортизацию используемого программного обеспечения.

***Требования к сертификации и применению в информационных системах:***СЗИ должно соответствовать требованиям документов: «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) – по 4 уровню контроля, «Требования к средствам контроля съемных машинных носителей информации (ФСТЭК России, 2014)», «Профиль защиты средств контроля съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ» (ФСТЭК России 2012), «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016), «Средства вычислительной техники. Защита от несанкционированного доступа к информации (Гостехкомиссия России, 1992) – по 5 классу защищенности». СЗИ должно допускать использование в следующих информационных системах:* автоматизированные системы - до класса 1Г (включительно);
* государственные информационные системы – до 1 класса защищенности (включительно);
* информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно);
* автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно).

СЗИ должно поддерживать защиту систем терминального доступа, а также допускать применение для защиты не только физических компьютеров, но и виртуальных машин.***Требования к операционной платформе и аппаратной части:**** СЗИ должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы):
	+ Windows 10;
	+ Windows 8.1;
	+ Windows 7 SP1;
	+ Windows Server 2019;
	+ Windows Server 2016
	+ Windows Server 2012/2012 R2;
	+ Windows Server 2008 R2 SP1.
* Должна быть возможность установки СЗИ по произвольному пути.
* СЗИ должно поддерживать работу и обеспечивать защиту в системах терминального доступа, построенных на базе терминальных служб сетевых ОС MS Windows или ПО Citrix.
* СЗИ должно поддерживать работу на виртуальных машинах, функционирующих в системах виртуализации, построенных на базе гипервизоров VMwareESX(i) и MicrosoftHyper-V.
* СЗИ должно поддерживать работу с технологией PersonalvDiskCitrixXenDesktop.
* СЗИ с централизованным управлением должно функционировать совместно с MicrosoftActiveDirectory;
* СЗИ должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ.
* СЗИ не должно требовать при развертывании модификации топологии локальной вычислительной сети.
* СЗИ должно иметь в составе дистрибутива драйвера для поддержки аппаратных идентификаторов.
* В инфраструктуре должно быть в наличии устройство, считывающее DVD (для чтения установочного диска – хотя бы на одном компьютере в информационной системе).

**Требования к функциональности СЗИ:**СЗИ должно выполнять следующие функции по защите информации:* Контроль входа пользователей в систему и работа пользователей в системе:
	+ проверка пароля пользователя при входе в систему;
	+ поддержка аппаратных средств аутентификации:

- идентификаторы iButton (типы DS1992 — DS1996);- USB-ключи eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta PKI/ГОСТ, JaCarta ГОСТ Flash, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCartaSF/ГОСТ, JaCartaPRO, JaCarta-2 PRO/ГОСТ, JaCartaWebPass, JaCarta-2 SE, JaCartaU2F, JaCartaLT, RutokenS, Rutoken ЭЦП, Rutoken ЭЦП 2.0, Rutoken ЭЦП Touch, Rutoken ЭЦП PKI, Rutoken ЭЦП Flash 2.0, Rutoken ЭЦП Bluetooth, RutokenLite, ESMARTToken, ESMARTToken ГОСТ, ESMARTTokenD.- смарт-карты eTokenPRO, eTokenPRO (Java), JaCartaPKI, JaCarta ГОСТ, JaCarta-2 PKI/ГОСТ, JaCartaPRO, JaCarta-2 PRO/ГОСТ, Rutoken ЭЦП, Rutoken ЭЦП 2.0, RutokenLite, ESMARTToken, ESMARTToken ГОСТ, ESMARTTokenD, с любыми совместимыми USB-считывателями;* + возможность блокировки сеанса работы пользователя при отключении персонального идентификатора;
	+ возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI);
	+ однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI);
	+ возможность блокирования входа в систему локальных пользователей;
	+ возможность блокирования операций вторичного входа в систему в процессе работы пользователей;
	+ возможность блокировки сеанса работы пользователя по истечении интервала неактивности;
	+ возможность управления политикой сложности паролей;
	+ поддержка возможности входа в систему по сертификатам;
	+ возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей;
	+ возможность оповещения пользователя о последнем успешном входе в систему;
	+ возможность выдачи пользователю предупреждения в виде сообщения о том, что в информационной системе реализованы меры защиты информации.
* Избирательное (дискреционное) управление доступом:
	+ возможность назначения прав доступа на файлы, каталоги, принтеры, устройства;
	+ возможность наследования прав доступа для файлов, каталогов и устройств;
	+ возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту.
* Полномочное (мандатное) управление доступом:
	+ возможность заведения в системе не менее 10 уровней конфиденциальности;
	+ возможность выбора уровня конфиденциальности сессии для пользователя;
	+ возможность назначения мандатных меток файлам, каталогам, внешним устройствам, принтерам, сетевым интерфейсам;
	+ возможность изменения количества мандатных меток в системе и их названий;
	+ контроль потоков конфиденциальной информации в системе;
	+ возможность контроля потоков информации в системах терминального доступа при передаче информации между клиентом и сервером по протоколу RDP.
* Контроль вывода конфиденциальных данных на печать:
	+ возможность ограничить перечень мандатных меток информации для печати на заданном принтере;
	+ теневое копирование информации, выводимой на печать:
		- должна быть возможность поиска по именам файлов, сохраненных в хранилище теневых копий;
		- должна быть возможность поиска по содержимому файлов, сохраненных в хранилище теневых копий. Должна обеспечиваться поддержка форматов, поддерживаемых компонентом WindowsSearch.
	+ автоматическая маркировка документов, выводимых на печать;
	+ управление грифами (видом маркировки) при печати конфиденциальных и секретных документов. При этом должна быть возможность задать:
		- отдельный вид грифа для каждой мандатной метки;
		- отдельный вид маркировки для первой страницы документа;
		- отдельный вид маркировки для последней страницы документа;
		- вид маркировки для оборота последнего листа;
	+ поддержка функции печати в файл;
	+ поддержка управления запретом перенаправления принтеров в терминальных (RDP) сессиях.
* Контроль аппаратной конфигурации компьютера и подключаемых устройств:
	+ Должны контролироваться следующие устройства:
		- последовательные и параллельные порты;
		- локальные устройства;
		- сменные, физические и оптические диски;
		- программно реализованные диски;
		- USB-устройства;
		- PCMCIA-устройства;
		- IEEE1394 (FireWire)- устройства;
		- устройства, подключаемые по шине SecureDigital.
	+ Должна быть возможность задать настройки контроля на уровне шины, класса устройства, модели устройства, экземпляра устройства.
	+ Должен осуществляться контроль неизменности аппаратной конфигурации компьютера с возможностью блокировки при нарушении аппаратной конфигурации.
	+ Должна быть возможность присвоить устройствам хранения информации мандатную метку. Если метка устройства не соответствует сессии пользователя – работа с устройством хранения должна блокироваться.
	+ Должна быть возможность группового добавления устройств в подсистему контроля устройств без подключения устройства к компьютеру.
	+ Должен осуществляться контроль вывода информации на внешние устройства хранения с возможностью теневого копирования отчуждаемой информации:
		- должна быть возможность поиска по именам файлов, сохраненных в хранилище теневых копий;
		- должна быть возможность поиска по содержимому файлов, сохраненных в хранилище теневых копий. Должна обеспечиваться поддержка форматов, поддерживаемых компонентом WindowsSearch.
	+ В инфраструктуре виртуальных рабочих станций (VDI) должны контролироваться устройства, подключаемые к виртуальным рабочим станциям с рабочего места пользователя.
	+ При терминальном подключении (RDP) должна быть возможность управления запретом подключения устройств, COM- и LPT-портов, локальных дисков и PnP-устройств.
* Контроль сетевых интерфейсов:
	+ Должна быть возможность включения/выключения явно заданного сетевого интерфейса или интерфейса, определяемого типом – Ethernet, WiFi, IrDA, Bluetooth, FireWire (IEEE1394).
	+ Должна быть возможность управления сетевыми интерфейсами в зависимости от уровня сессии пользователя.
* Создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера. При этом должны контролироваться исполняемые файлы (EXE-модули), файлы загружаемых библиотек (DLL-модули), запуск скриптов по технологии ActiveScripts.
	+ Список модулей, разрешенных для запуска, должен строиться:
		- с помощью явного указания модулей;
		- по информации об установленных на компьютере программах;
		- по зависимостям исполняемых модулей;
		- по ярлыкам в главном меню;
		- по событиям журнала безопасности.
* Контроль целостности файлов, каталогов, элементов системного реестра:
	+ Должна быть возможность проведения контроля целостности в процессе загрузки ОС, в фоновом режиме при работе пользователя.
	+ Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов.
	+ Должна быть возможность восстановления исходного состояния контролируемого объекта.
	+ Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП.
	+ При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ.
* Изоляция программных модулей и контроль доступа к буферу обмена и операциям перетаскивания (drag-and-drop) для изолированных модулей.
* Автоматическое затирание удаляемой информации на локальных и сменных дисках компьютера при удалении пользователем конфиденциальной информации с возможностью настройки количества проходов затирания информации.
* Автоматическое затирание оперативной памяти компьютера с возможностью настройки количества проходов затирания информации.
* Затирание информации на локальных и сменных дисках по команде пользователя.
* Возможность настройки количества проходов затирания информации отдельно для локальных дисков, съемных носителей, оперативной памяти.
* Затирание данных и имен файлов, каталогов при удалении информации.
* Возможность добавления объектов файловой системы в исключения подсистемы затирания данных.
* Возможность управления запретом передачи буфера обмена в терминальную (RDP) сессию.
* Шифрование контейнеров:
	+ Должна обеспечиваться возможность создания зашифрованных контейнеров (криптоконтейнеров) с возможностью подключения их к системе как виртуальных дисков.
	+ Вся информация, размещаемая в контейнере, должна шифроваться по алгоритму ГОСТ 28147-89.
	+ Ключевая информация для обеспечения шифрования и расшифровки данных в криптоконтейнерах должна размещаться в аппаратных идентификаторах или на съемном USB-носителе.
	+ Должна быть возможность выбора размера криптоконтейнера при его создании.
	+ Должна поддерживаться возможность автоматического и ручного подключения криптоконтейнера по команде пользователя.
	+ Доступ к криптоконтейнерам должен регулироваться дискреционными правилами разграничения доступа.
* Защита сетевого взаимодействия и фильтрация трафика:
	+ Должны быть механизмы аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.
	+ Должны удостоверяться субъекты доступа (пользователи и компьютеры) и защищаемые объекты (компьютеры).
	+ Механизмы должны быть защищены от прослушивания, попыток подбора и перехвата паролей, подмены защищаемых объектов, подмены MAC- и IP-адресов.
	+ Должны быть предусмотрены механизмы защиты установленных сетевых соединений между субъектами доступа (пользователями и компьютерами) и защищаемыми объектами (серверами и информационными системами) на основе открытых стандартов протоколов семейства IPsec, которые позволяют контролировать аутентичность и целостность передаваемых данных.
	+ Должна быть предусмотрена настройка режима защиты сетевого взаимодействия, при этом должны быть предусмотрены следующие режимы защиты:
		- соединение без защиты;
		- маркируется каждый пакет;
		- подписывается заголовок каждого пакета;
		- подписывается каждый пакет целиком.
	+ Должна быть возможность ограничивать сетевые соединения по правилам фильтрации:
		- на уровне отдельных протоколов из стека TCP/IP;
		- на уровне параметров протоколов стека TCP/IP;
		- на уровне параметров служебных протоколов стека TCP/IP;
		- на уровне периодов времени;
		- на уровне пользователей или групп пользователей;
		- на уровне параметров прикладных протоколов;
		- на уровне исполняемого файла/процесса;
		- на уровне сетевого адаптера.
	+ Должна быть возможность осуществлять фильтрацию команд, параметров и последовательностей команд, а также обеспечивать блокировку мобильного кода.
	+ Должна быть возможность маркировки сетевого трафика метками конфиденциальности.
	+ Должен быть предусмотрен выбор действий для определения реакции системы на срабатывание правил фильтрации:
		- регистрация информации в журнале;
		- звуковая сигнализация;
		- запуск программы или сценария.
* Функциональный контроль ключевых компонентов системы.
* Регистрация событий безопасности в журнале.
	+ Должна быть возможность формирования отчетов по результатам аудита.
	+ Должна быть возможность поиска и фильтрации при работе с данными аудита.
* возможность организации федерации – иерархической структуры лесов доменов безопасности. В федерацию можно добавлять леса доменов безопасности на основе несвязанных лесов доменов Windows AD.
* возможность централизованного развертывания СЗИ от НСД с использованием SystemCenterConfigurationManager 2012, 2016.
* Защита от локального администратора, обеспечивающая разграничение прав и привилегий между Администратором безопасности и Администратором IT на локальное управление СЗИ.
* возможность задания временного интервала блокировки компьютера (в минутах) в случае достижения установленного максимального количества попыток ввода неправильного пароля.

***Требования к централизованному управлению в доменной сети:***СЗИ должно предоставлять следующие возможности по управлению системой: * Отображение структуры доменов, организационных подразделений, серверов безопасности и защищаемых компьютеров.
* Динамическое отображение состояния каждого защищаемого компьютера с учетом критичности состояния с точки зрения системы защиты.
* Отображение тревог, происходящих на защищаемых компьютерах, возможность задать признак того, что тревога обработана администратором безопасности.
* Разделение тревог по уровням критичности события и важности отдельных защищаемых компьютеров.
* Возможность настройки отображения диаграмм (детализации, цветовой гаммы), добавления, удаления, перемещения диаграмм на панели мониторинга.
* Выполнение оперативных команд для немедленного реагирования на инциденты безопасности (заблокировать работу пользователя, выключить компьютер).
* Оперативное управление защищаемыми компьютерами, возможность централизованно изменить параметры работы защищаемого компьютера.
* Возможность создавать централизованные политики безопасности, распространяемые на разные (заданные) группы защищаемых компьютеров.
* Централизованный сбор журналов безопасности с защищаемых компьютеров, их хранение, возможность обработки и архивирования.
* Анализ собранных журналов на наличие заданных угроз безопасности с поддержкой редактирования правил детектирования угроз.
* Возможность инвентаризации объектов файловой системы компьютера с последующим сохранением отчета в виде эталонного паспорта. Возможность сравнения нового паспорта с эталонным, возможность переопределения эталона.
* Возможность создания отчетов о настройках системы, установленных программах, зарегистрированных аппаратных средствах аутентификации.
* Возможность создания шаблонов политик:
	+ возможность создания шаблона по настроенным политикам СЗИ на компьютере;
	+ возможность проверки соответствия настроенных политик СЗИ на компьютере с выбранным шаблоном;
	+ возможность распространения (применения) шаблонов политик на компьютер или группу компьютеров.
* Централизованное управление в сложной доменной сети (domaintree) должно функционировать по иерархическому принципу, при этом система должна позволять:
	+ распространить настройки, заданные для сервера безопасности, на все подчиненные компьютеры (в том числе – по иерархии серверов);
	+ посмотреть состояние и выполнить команду на любом компьютере, подчиненном серверу безопасности (в том числе – по иерархии серверов);
	+ создавать иерархию серверов безопасности с не менее чем 3 уровнями вложенности.
* Создавать домены безопасности в территориально распределенной сети, при этом должна предоставляться возможность делегирования административных полномочий лицам, ответственным за подразделения (домены безопасности).
* возможность централизованного управления защищаемыми компьютерами из дочерних лесов доменов безопасности в структуре лесов доменов безопасности, организованной на основе несвязанных лесов доменов Windows AD.
* поддержка групповых операций в Контроле устройств (выбор нескольких устройств в рамках одного класса и назначение параметров контроля/доступа на выбранные устройства).
 |  | Наличие |
| Установка, настройка и адаптация средства защиты информации от несанкционированного доступа |  | Наличие |
| **ПО ViPNetIDSHS(базовая лицензия)\*\*** | **1** | **ПО ViPNetIDSHS (базовая лицензия)** |  |  |
| Состав: |  |  |
| - неисключительных прав на использование программного обеспечения ViPNet IDS HS (базовая лицензия) в составе один ViPNetIDSHSserverи десять ViPNetIDSHSagent |  | Наличие |
| Установка и настройка осуществляется в соответствие с эксплуатационной документацией к средствам защиты информации, а также для нейтрализации актуальных угроз безопасности и выполнения мер по защите информации предусмотренных нормативно-правовыми актами РФ. |  | Наличие |
| Установочный комплект программного обеспечения ViPNet IDS HS\* | Шт. | Не менее 1 |
| **Разработка технических документов на систему защиты информации** | **1** | **Разработка технических документов на систему защиты информации** |  |  |
| Состав  |  |  |
| - модель угроз безопасности включая модель нарушителей безопасности информации |  | Наличие |
| - техническое задание ан построение системы защиты информации  |  | Наличие |
| - программа и методика аттестационных испытаний по требования безопасности информации  |  | Наличие  |
| - технический паспорт информационной системы  |  | Наличие |
| **Проведение аттестационных испытаний на ИС по требованиям безопасности** | **1** | Состав  |  |  |
| - протокола испытаний |  | Наличие |
| - заключения по результатам испытаний |  | Наличие  |
| - аттестата соответствия ИС требованиям безопасности информации |  | Наличие  |
| **ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ**  |  | Исполнитель должен обладать лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации со следующими видами деятельности:* работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации;
* услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).
 |  | Наличие |
| Исполнитель должен обладать ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя). |  | Наличие |

\*- эквивалент не допустим из-за необходимости совместимости с имеющимися средствами защиты у Заказчика

\*\* - эквивалент недопустим в связи с необходимостью выполнения пункта 3.3.1 Технических условий на подключение медицинских организаций к государственной информационной системе «Республиканская медицинская информационно-аналитическая система Республики Башкортостан» технологией

 Требования к Исполнителю:

1. отсутствие у участника закупки - физического лица либо у руководителя, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа, или главного бухгалтера юридического лица - участника закупки судимости за преступления в сфере экономики и (или) преступления, предусмотренные [статьями 289](https://www.consultant.ru/document/cons_doc_LAW_444861/7cb5d9b7f75fd72853e0610988cc9f6fdd08802e/#dst101897), [290](https://www.consultant.ru/document/cons_doc_LAW_444861/6411e005f539b666d6f360f202cb7b1c23fe27c3/#dst2054), [291](https://www.consultant.ru/document/cons_doc_LAW_444861/0108932a3c6234f73590b25799588ada492deb23/#dst2072), [291.1](https://www.consultant.ru/document/cons_doc_LAW_444861/a74ca4364cb5aa0d95db2b7636907af350ab52c8/#dst2086) Уголовного кодекса Российской Федерации (за исключением лиц, у которых такая судимость погашена или снята), а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся объектом осуществляемой закупки, и административного наказания в виде дисквалификации;
2. - участник закупки - юридическое лицо, которое в течение двух лет до момента подачи заявки на участие в закупке не было привлечено к административной ответственности за совершение административного правонарушения, предусмотренного [статьей 19.28](https://www.consultant.ru/document/cons_doc_LAW_460025/f61ff313afecf81a91a43d729c2df55c1d6a1533/#dst2620) Кодекса Российской Федерации об административных правонарушениях;
3. -участник закупки не является офшорной компанией, не имеет в составе участников (членов) корпоративного юридического лица или в составе учредителей унитарного юридического лица офшорной компании, а также не имеет офшорных компаний в числе лиц, владеющих напрямую или косвенно (через юридическое лицо или через несколько юридических лиц) более чем десятью процентами голосующих акций хозяйственного общества либо долей, превышающей десять процентов в уставном (складочном) капитале хозяйственного товарищества или общества;
4. - участник закупки не является иностранным агентом;
5. -участник закупки не является юридическим лицом, либо полномочным представителем юридического лица (филиал ставший самостоятельным юр лицом, после 22.02.2022 г. – но зависимый от импорта товаров вне пределов Евразийского экономического союза) поддерживающего санкционный режим в отношении РФ;
6. -отсутствие между участником закупки и заказчиком конфликта интересов, под которым понимаются случаи, при которых руководитель заказчика, член комиссии по осуществлению закупок, руководитель контрактной службы заказчика, контрактный управляющий состоят в браке с физическими лицами, являющимися выгодоприобретателями, единоличным исполнительным органом хозяйственного общества (директором, генеральным директором, управляющим, президентом и другими), членами коллегиального исполнительного органа хозяйственного общества, руководителем (директором, генеральным директором) учреждения или унитарного предприятия либо иными органами управления юридических лиц - участников закупки, с физическими лицами, в том числе зарегистрированными в качестве индивидуального предпринимателя, - участниками закупки либо являются близкими родственниками (родственниками по прямой восходящей и нисходящей линии (родителями и детьми, дедушкой, бабушкой и внуками), полнородными и неполнородными (имеющими общих отца или мать) братьями и сестрами), усыновителями или усыновленными указанных физических лиц. Под выгодоприобретателями для целей настоящей статьи понимаются физические лица, владеющие напрямую или косвенно (через юридическое лицо или через несколько юридических лиц) более чем десятью процентами голосующих акций хозяйственного общества либо долей, превышающей десять процентов в уставном капитале хозяйственного общества;
7. - отсутствии сведений об участниках закупки в реестре недобросовестных поставщиков, предусмотренном статьей 5 Федерального закона «О закупках товаров, работ, услуг отдельными видами юридических лиц», и (или) в реестре недобросовестных поставщиков, предусмотренном Федеральным законом «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
1. [↑](#footnote-ref-2)