**Техническое задание**

**1.1. Наименование объекта закупки:** Оказание услуг по поставке средств защиты информации

**1.2. Описание объекта закупки:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Назначение продукта/модуля** | **КТРУ** | Кол-во |
| 1 | Программное средство защиты от несанкционированного доступа | СЗИ НСД должна представлять собой программный комплекс средств защиты информации в операционных системах (ОС) семейства Windows с возможностью подключения аппаратных идентификаторов.СЗИ НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 в многопользовательском режиме их эксплуатации.СЗИ НСД должна поддерживать 32- и 64-битные версии операционных систем.СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go.СЗИ НСД должна быть сертифицирована на соответствие требованиям руководящих документов к 5-му классу защищенности от НСД для СВТ (РД СВТ, Гостехкомиссия России, 1992) и 4-му уровню доверия («Требования по безопасности информации, устанавливающие уровни доверия к СТЗИ и СОБИТ», ФСТЭК России, 2020), разрабатываться и производиться на основании лицензии федеральных органов, имеющих полномочия в указанной сфере. Модуль СКН должен быть сертифицирован на соответствие требованиям ФСТЭК России к средствам контроля съемных машинных носителей информации по 4-му классу защиты в соответствии с профилем защиты средств контроля подключения съемных машинных носителей информации (ИТ.СКН.П4.ПЗ).СЗИ НСД может быть использована:* при создании защищенных автоматизированных систем до класса защищенности 1Г включительно;
* в государственных информационных системах до 1 класса защищенности включительно;
* в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно;
* в информационных системах персональных данных до 1 уровня защищенности включительно;
* при защите значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно.

СЗИ НСД должна обеспечивать:регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере. Возможность автоматического блокирования неактивных учетных записей пользователей;идентификацию и проверку подлинности пользователей при входе в ОС. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность задать расписание работы пользователей. Возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность аппаратного идентификатора конкретному пользователю. Возможность запрета повторного использования идентификатора. Возможность ограничения количества неуспешных попыток входа и блокирования устройства. Возможность автоматизированно сохранять авторизационные данные пользователя в системном кэше ОС при использовании (установке) СЗИ НСД. Поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows. Поддержку аутентификации пользователей с применением биометрии и токенов JaCarta PKI/BIO;реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам;возможность автоматического выбора аппаратного идентификатора в окне авторизации при входе в ОС;возможность настройки принудительной двухфакторной аутентификации для учетной записи с правами администратора и/или пользователя;возможность средствами СЗИ НСД выполнить настройку периода действия учетной записи;возможность настройки предупреждения пользователя до входа в систему о том, что в информационной системе реализованы меры по обеспечению безопасности информации;возможность при создании учетной записи выбрать тип учетной записи (внутренний, внешний, системный, приложение, гостевой, временный);независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), реестру, сети, съемным носителям информации. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных;контроль аппаратной конфигурации компьютера и следующих подключаемых устройств:* + Android-устройств;
	+ iOS-устройств;
	+ Bluetooth-устройств;
	+ DVD- и CD-ROM-дисководов;
	+ устройств HID, MTD, PCMCIA, IEEE 1394, Secure Digital;
	+ USB-контроллеров;
	+ беспроводных устройств (Wireless Communication Devices);
	+ биометрических устройств;
	+ дисководов магнитных дисков;
	+ звуковых, видео- и игровых устройств;
	+ инфракрасных устройств (IrDA);
	+ контроллеров магнитных дисков;
	+ ленточных накопителей;
	+ модемов;
	+ переносных устройств;
	+ портов (COM и LPT);
	+ сенсоров;
	+ сетевых адаптеров;
	+ сканеров и цифровых фотоаппаратов;
	+ принтеров;
	+ съемных носителей информации (CD-ROM, FDD, USB-Flash-накопителей).
* контроль устройств, подключаемых к терминальному серверу с RDP‑клиентов (контроль перенаправления устройств);
* предотвращение утечки информации с использованием съемных носителей информации. СЗИ НСД должна позволять разграничивать доступ как к отдельным типам носителей, так и к конкретным экземплярам;
* возможность запретить запуск (без команды пользователя) ПО, используемого для взаимодействия со съемными носителями информации;
* возможность запретить установку драйверов съемных носителей информации;
* преобразование информации:
* при работе с виртуальными дисками (преобразование выполняется незаметно для пользователя);
* при создании преобразованных файлов-контейнеров, используемых для хранения информации на внешних носителях или для передачи по различным каналам связи.

блокировку виртуальных дисков с преобразованной информацией при отключении аппаратного идентификатора;сохранение теневых копий файлов, записываемых на съемные носители;автоматическое ограничение доступа к теневой копии, сделанной СЗИ НСД при копировании документа, содержащего информацию ограниченного доступа, на сменный машинный носитель;использование дискреционного принципа контроля доступа, обеспечивающего доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа);возможность ограничивать средствами СЗИ НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа);регистрацию и учет (аудит) действий пользователей независимыми от ОС средствами (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки и автоматической архивации по истечении установленного интервала времени; расширенные возможности аудита печати: печать документов с возможностью добавления штампа (произвольного или по ГОСТ), возможность сохранения теневых копий распечатываемых документов, разграничение доступа пользователей к печати и нанесению штампов;возможность добавления произвольного комментария к зарегистрированным событиям НСД;возможность экспорта журналов событий в syslog, возможность настройки кодировки экспортируемых в syslog событий;возможность организации замкнутой программной среды (ЗПС) и различные способы ее настройки;блокировку доступа к файлам по расширению;возможность разграничения доступа к буферу обмена;возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов);возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений. Возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности;очистку остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Возможность определения метода зачистки. Контроль зачистки при полной зачистке логического диска. Очистку данных сеанса пользователя в оперативной памяти за счет запрета смены пользователя без перезагрузки;возможность проверки цифровой подписи объектов файловой системы, находящихся под контролем целостности, при их обновлении;выполнение регистрации действий по зачистке остаточной информации;самодиагностика основных функциональных возможностей СЗИ НСД и сохранение информации в виде отчета;возможность сохранения конфигурации для последующего восстановления СЗИ НСД; возможность настройки всех параметров СЗИ НСД из единой консоли администрирования;возможность создания отчета по назначенным правам, формирование паспорта программного обеспечения, установленного на ПЭВМ, формирование паспорта аппаратной части ПЭВМ;ведение двух копий программных средств защиты информации и возможность возврата к настройкам по умолчанию;возможность сигнализации администратору безопасности о следующих инцидентах безопасности (ситуациях сбоя функционирования и ситуациях несанкционированного доступа на клиентских рабочих станциях):* + нарушение контроля целостности объекта;
	+ попытка работы после блокировки при нарушении целостности;
	+ попытка входа на клиентскую рабочую станцию с неправильным паролем;
	+ блокировка пользователя после многократного ввода неправильного пароля;
	+ СЗИ НСД на клиенте не отвечает (возможная причина - несанкционированная деактивация системы защиты);
	+ клиент недоступен долгое время (с возможностью задания периода времени);
	+ попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами.

централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учетными записями пользователей, политиками, правами пользователей, преобразованными съемными носителями информации. Должна поддерживаться многоуровневая иерархия групп компьютеров и наследование установленных параметров. Также этим модулем должен осуществляться периодический сбор журналов со всех защищенных рабочих станций. Возможность блокировки компьютера, завершения сеанса работы пользователя по команде администратора;Должен быть реализован модуль контроля подключения съемных машинных носителей информации (СКН).Модуль СКН должен обеспечивать:контроль использования интерфейсов ввода/вывода средств вычислительной техники, подключения внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации;возможность назначения прав доступа к конкретному накопителю;возможность установить описание для сменного накопителя.Реализация СЗИ НСД должна быть полностью программной с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, а также аппаратных идентификаторов: * USB-флэш-накопители;
* электронные ключи Touch Memory (iButton);
* HID Proximity-карты;
* USB-ключи Aladdin eToken Pro/Java;
* смарт-карты Aladdin eToken Pro/SC;
* USB-ключи и смарт-карты Рутокен (Rutoken), Рутокен ЭЦП, Рутокен ЭЦП 2.0;
* USB-ключи и смарт-карты JaCarta, JaCarta-2, JaCarta PRO, JaCarta LT, JaCarta PKI/BIO;
* USB-ключи и смарт-карты ESMART;
* NFC-метки и смарт-карты семейства MIFARE.

Поставка СЗИ НСД должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием всех необходимых модулей и требуемого количества лицензий по каждому модулю. Варианты формулировок:* неисключительное право на использование СЗИ (НСД, СКН) (программное обеспечение)
 | 62.01.29.000-00000004 | 25 шт. |
| 2 | Программное средство антивирусной защиты | Программные средства Системы должны обеспечивать определение угроз следующих типов:* классических вирусов;
* троянских программ;
* руткитов;
* сетевых червей;
* рекламных программ;
* программ автодозвона на платные сайты;
* потенциально опасных приложений;
* прочих вредоносных программ.

Антивирусная защита должна обеспечивать:* обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п.;
* обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками;
* обнаружение вирусов внутри контейнеров и архивных файлов формата ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (включая NRG, образы с нестандартным форматом сектора и не имеющие сигнатур), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER с зашифрованными контейнерами и т.д. без ограничений на уровень вложенности проверяемых объектов;
* обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME);
* обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т.д.);
* антивирусную проверку файлов и объектов, имеющих формат Smart Install Maker (SIM); DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); INNO SETUP (5.3.9 и выше); SETUP FACTORY (линейки 7,8); XENOCODE; TARMA INSTALL (линейка 3); XZ (UNIX); COMPRESS; SQUAHFS; CHILKAT ZIP; пакеты LHA (AWARD BIOS);
* антивирусную проверку в самораспаковывающихся архивах: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy;
* проверку исполняемых файлов упакованных следующими упаковщиками: PELOCK, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, а также почтовых файлов Mozilla Thunderbird- вне зависимости от их размера;
* разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF;
* защиту от вредоносных программ, принадлежащих семействам вредоносных программ, информация о которых имеется в антивирусных базах, созданных после занесения соответствующей информации в антивирусные базы и еще не попавших на анализ в антивирусные лаборатории - как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;
* обнаружение вредоносных объектов в HTML- и PDF-документах, включая обфусцированные эксплойты в JavaScript, находящиеся в документах данных типов. Возможность извлечения и анализа «невидимых» IFRAME-элементов. Возможность извлечения для проверки скриптов любой сложности и снятие с них защиты;
* обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA);
* обнаружение угроз направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля

Используемое антивирусное ядро:* не должно допускать снижение скорости проверки при увеличении размера антивирусных баз;
* в связи с возможностью исчерпания ресурсов ОС (в том числе места на диске, памяти) в ходе обработки специальным образом сформированных архивов автоматически выбирать уровень анализа упакованных объектов, а также механизм уменьшения размера промежуточных файлов. При выборе уровня анализа должен учитываться уровень загрузки системы
* в целях ускорения проверки архивов и упакованных файлов должно обеспечивать опознание вредоносных программ без запуска распаковщика;
* должно обеспечивать защиту от так называемых «почтовых бомб»;
* должно обеспечивать работу с файлами размером как менее, так и больше 2 ГБ;
* должно поддерживать работу с дисками с LBA-адресацией;
* в целях исключения «утечки» оперативной памяти должно использовать механизм распределения динамической памяти уровня антивирусного ядра.

**Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows**Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:* осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях.

Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствие требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна обеспечивать защиту рабочих станций под управлением операционных систем:* + - * Microsoft Windows XP Professional;
			* Microsoft Windows 7;
			* Microsoft Windows 8.1;

Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур.Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов.Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав.В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:* + - * поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
			* непрерывное фоновое сканирование в целях нейтрализации активных угроз
			* проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;
			* проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
			* блокировку опасных макросов VBA в реальном времени;
			* защиту от вредоносных сценариев, загружаемых с Web-страниц;
			* защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана;
			* проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО;
			* защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных носителей информации, локальным файлам и каталогам, сайтам в сети Интернет;
			* ограничения доступа к сети Интернет или к компьютеру в определенный момент времени по расписанию
			* помещение найденных зараженных файлов в специальное место на жестком диске -«карантин»;
			* просмотр местоположения станций и серверов на карте, если заданы географические координаты станции
			* автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
			* запуск задач по расписанию и/или сразу после загрузки операционной системы;
			* возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке.

Система защиты рабочих станций должна обеспечивать проверку протоколов: * + - HTTP;
		- IMAP, SMTP, POP3 независимо от используемого почтового клиента;
		- NNTP (только проверка на вирусы), независимо от почтового клиента.

Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством:* + - антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
		- проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.

В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.Система должна обеспечивать защиту от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) с помощью превентивной защиты, отслеживающей попытки внедрения вредоносных файлов В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.**Требования по комплектности поставки**В состав Системы должны входить:* + - * программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания;
			* обновляемые базы данных сигнатур всевозможных вредоносных программ.

Комплект поставки должен содержать:* + - * необходимый набор серийных номеров либо ключевых файлов;
			* дистрибутив Системы;
			* файлы эксплуатационной документации в формате pdf (Adobe Acrobat Reader), в том числе руководство пользователя (администратора). Поставляемая документация должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

Комплект поставки, сертифицированный ФСТЭК России, должен содержать:* DVD-диск в фирменном конверте, содержащий верифицированные дистрибутивы сертифицированных продуктов
* документацию и материалы в формате PDF для настройки поставляемого программного обеспечения в соответствии с сертифицированными параметрами, приведенными в технической документации;
* формуляр, содержащий эталонные значения контрольных сумм сертифицированных продуктов;
* лицензионный сертификат, удостоверяющий законное приобретение программного изделия;
* заверенную копию сертификата соответствия ФСТЭК России.
 | 62.01.29.000-00000009 | 1 усл. ед. |
| 3 | Программное средство криптографической защиты | **Требования к реализации криптографических стандартов**Применяемое средство криптографической защиты информации (средство электронной подписи) должно обеспечивать применение электронной подписи (ЭП) и шифрования в соответствии с нормами действующего законодательства Российской Федерации и осуществлять выполнение следующих основных функций:* генерацию и управление ключевой информацией;
* формирование электронной подписи в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018) (в усиленном режиме формирование электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001 запрещено с 1 января 2020 года);
* подтверждение подлинности электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (ГОСТ 34.10-2012);
* подсчет значения хэш-функции в соответствии с ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018);
* шифрование и расшифрование данных в соответствии с ГОСТ 28147-89;
* формирование ключей электронной подписи и ключей проверки электронной подписи, а также ключей шифрования;
* идентификацию, аутентификацию, шифрование, имитозащиту TLS соединений;
* реализацию набора протоколов IPsec в соответствии с особенностями использования отечественных криптографических алгоритмов.

**Требования к реализации программного интерфейса встраивания**Средство криптографической защиты информации (средство электронной подписи) должно соответствовать криптографическому интерфейсу компании Microsoft - Cryptographic Service Provider (CSP).Встраивание средства криптографической защиты информации (средства электронной подписи) в прикладную информационную систему должно предусматривать возможность:* Применения в операционных системах семейства Microsoft Windows интерфейса функций:
* CAPICOM;
* Certificate Enrollment Control;
* Certificate Enrollment API;
* Certificate Services.
* вызова функций средства криптографической защиты информации (средства электронной подписи);
* применения в стандартном прикладном программном обеспечении операционных систем семейства Microsoft Windows MS Outlook Express; MS IE; MS IIS; Outlook, и т.д. (для поддержки MS Office Word, Excel может требоваться дополнительное ПО от разработчика средства криптографической защиты информации (средства электронной подписи)).

**Требования к алгоритмам, сертификатам открытых ключей и поддерживаемым форматам криптографических сообщений**Применяемое средство криптографической защиты информации (средство электронной подписи) должно реализовывать ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Информационная технология. Криптографическая защита информации. Блочные шифры», ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018) «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».Применяемое средство криптографической защиты информации (средство электронной подписи) должно реализовывать ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 и ГОСТ 28147-89 с учетом RFC 4357 «Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms», ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 34.10-2018, ГОСТ 34.10-2018. Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать сертификаты открытых ключей стандарта X.509v3 согласно RFC 5280 «Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile» с учетом RFC 4491 «Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile», а также документа Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), «Техническая спецификация. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509».Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать формат криптографических сообщений согласно RFC 3852 «Cryptographic Message Syntax (CMS)» с учетом RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)», а также документа Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS».Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать возможность создания форматов криптографических сообщений типа CAdES в соответствии с ETSI TS 101 733 (Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)): * формата CAdES-BES;
* формата CAdES–T;
* формата СAdES-X Long Type 1,

а также формата XML DSign для формирования электронной подписи в XML при встраивании в прикладные информационные системы с использованием программных библиотек (SDK) от разработчика средства криптографической защиты информации (средства электронной подписи). Отдельные компоненты таких программных библиотек могут лицензироваться дополнительно.**Требования к составу**Комплектация исполнения средства криптографической защиты информации (средства электронной подписи) должна включать:* Модуль сетевой аутентификации TLS, обеспечивающий реализацию сетевого протокола TLS с использованием российских криптографических стандартов (возможности модуля TLS определяются типом лицензии на средство криптографической защиты информации (средство электронной подписи))

**Функциональные требования**Средство криптографической защиты информации (средство электронной подписи) должно предоставлять программный интерфейс для выполнения следующих основных функций:* формирование электронной подписи на рабочем месте пользователя;
* подтверждение подлинности электронной подписи на серверах и рабочих местах пользователей;
* подсчет значения хэш-функции данных на серверах и рабочих местах пользователей;
* шифрование и расшифрование данных на рабочем месте пользователя и (или) сервере (в зависимости от типа лицензии);
* формирование ключей электронной подписи и ключей проверки электронной подписи на рабочем месте пользователя и (или) сервере (в зависимости от типа лицензии);
* поддержка аппаратных средств визуализации подписываемой информации, включая форматы подписи таких аппаратных устройств (типа Рутокен PinPad)

Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать выполнение следующих сервисных функций:* встраивание средства криптографической защиты информации в прикладную информационную систему должно предусматривать возможность использования библиотеки SDK TLS в мобильные приложения без проведения исследований по оценке влияния ОС мобильных устройств на СКЗИ.
* установка личных сертификатов и ключей проверки электронной подписи на рабочем месте/сервере с обеспечением связи сертификата открытого ключа с соответствующим указанному сертификату закрытым ключом;
* копирование и удаление ключей электронной подписи;
* установка, изменение и удаление пароля на доступ к закрытому ключу.
* создание и проверка электронной подписи в формате CMS (присоединенной и отсоединенной) с использованием графического интерфейса пользователя;
* Установка параметров работы в режиме «Облачного провайдера», включая определение сетевых адресов подключения, установку сертификатов ключей проверки электронной подписи, хранящихся в «облачном токене».

Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать эксплуатацию на следующих операционных системах (иметь клиентскую лицензию):* Windows 7/8/8.1/10 (x86/x64).

**Требования к сертификации** Средство электронной подписи (средство криптографической защиты информации) должно быть сертифицировано или иметь положительное Заключение ФСБ России по требованиям:* К средствам электронной подписи;
* К средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, по классам КС1, КС2, КС3.

Классы защиты КС2, КС3 могут обеспечиваться с учетом доступности ОС для конкретного класса защиты.Класс защиты КС3 должен обеспечиваться для функционирования СКЗИ в среде следующих операционных систем:Windows 7/8/8.1/10/Server 2008 (x86, x64);Windows Server 2008 R2/2012/2012 R2/2016 (x64). | 62.01.29.000-00000013 | 25 шт. |

**Проект Договора**

**оказание услуг по поставке средств защиты информации**

|  |  |
| --- | --- |
| г. Вельск | «\_\_\_» ­­­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023г. |

Государственное автономное учреждение здравоохранения Архангельской области «Вельская стоматологическая поликлиника» (сокращенно – ГАУЗ АО «ВСП»), в лице главного врача Шестаковой Людмилы Николаевны, действующей на основании Устава, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Исполнитель», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующей (его) на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, именуемые совместно в дальнейшем «Стороны», на основании протокола рассмотрения Заявок на участие и подведение итогов в запросе котировок в электронном виде от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023 г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ заключили настоящий Договор о нижеследующем.

**1. Предмет Договора, срок, место оказания Услуги**

1.1. Исполнитель принимает на себя обязательства **оказание услуг по поставке средств защиты информации** (далее – Услуг) в соответствии с Приложением № 1 «Техническое задание» к настоящему Договору (далее – Приложение № 1 к Договору), а Заказчик обязуется принять и оплатить товар.

1.2. Срок оказания Услуги: начало оказания услуг: с 01.07.2023 г.; окончание оказания услуг: 31.12.2023 г.

1.3. Датой исполнения Исполнителем обязательств считается дата подписания Исполнителем и Заказчиком Акта оказанных услуг.

 1.4. Услуга оказывается Исполнителем по адресу Заказчика: 165150, Архангельская обл., г. Вельск, ул. Дзержинского, д.42

**2. Цена Договора**

2.1. Оплата стоимости поставленной по настоящему Договору Услуги производится в рублях.

2.2. Цена Услуги, указанного в пункте 1.1 настоящего Договора, определена протоколом рассмотрения Заявок от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_2023 г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.3. Цена настоящего Договора, составляет \_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) рубля \_\_\_ копеек, НДС не облагается (п. 2 ст. 346.14 гл. 26.2 Налогового кодекса Российской Федерации).

2.4. Цена Договора включает в себя стоимость Услуги, все расходы по оказанию Услуги, в том числе все сопутствующие расходы, уплачиваемые Исполнителем налоги, сборы и иные платежи.

2.5. Цена Договора является твердой, определяется на весь срок исполнения Договора и не может изменяться в ходе его исполнения, за исключением случаев, предусмотренных настоящим Договором.

2.6. Цена Договора может быть снижена по соглашению Сторон без изменения предусмотренных Договором объема Услуг, качества оказываемых услуг и иных условий исполнения Договора.

**3. Порядок расчетов**

3.1. Оплата Услуги осуществляется по цене, установленной Договором.

3.2.Моментом исполнения Заказчиком обязательства по оплате считается день списания денежных средств со счета Заказчика.

3.3.Оплата производится по безналичному расчету путем перечисления денежных средств на расчетный счет Исполнителя по факту исполнения обязательств по настоящему Договору в течение 10 (десяти) рабочих дней после подписания Сторонами Акта об оказании услуг, на основании счета, счета-фактуры при наличии финансирования.

3.4. Авансирование не предусмотрено.

**4. Права и обязанности сторон**

***4.1. Права и обязанности Заказчика:***

* + 1. Осуществлять контроль за количеством, качеством и объемом оказываемых услуг и проверять их на соответствие требованиям настоящего Договора. Требовать от Исполнителя надлежащего исполнения обязательств по настоящему Договору.
		2. При обнаружении в ходе оказания услуг отступлений от условий настоящего Договора, которые могут ухудшить качество оказываемых услуг, или иных недостатков, незамедлительно заявить об этом Исполнителю в письменной форме, назначив срок их устранения. Выявленные отступления от условий настоящего Договора фиксируются актом.
		3. В сроки и в порядке, которые предусмотрены настоящим Договором, с участием Исполнителя принять оказанные услуги, а при обнаружении отступлений от Договора, ухудшающих результат оказанных услуг, или иные недостатки в оказанных услугах немедленно заявить об этом Исполнителю, установив срок для их устранения.
		4. По завершению приемки сторонами оказанных услуг, Заказчик, при наличии зафиксированных фактов неисполнения и/или ненадлежащего исполнения Исполнителем обязательств по Договору, направляет Исполнителю уведомление с расчетом неустойки, для проведения зачета встречного однородного требования, в соответствии со ст. 410 ГК РФ.
		5. Оплатить Исполнителю оказанные услуги в размере и в сроки, предусмотренные Договором.

4.1.7. Заказчик вправе требовать от Исполнителя надлежащего исполнения обязательств в соответствии с Договором.

4.1.8. Заказчик вправе требовать представления надлежащим образом, оформленных отчетных и финансовых документов, подтверждающих исполнение обязательств в соответствии с Договором.

4.1.9. Запрашивать информацию о ходе и состоянии исполнения обязательств по Договору.

4.1.10. Для проверки представленных Исполнителем результатов, предусмотренных Договором, в части их соответствия условиям Договора, Заказчик вправе создавать комиссии, привлекать экспертов, экспертные организации.

***4.2. Права и обязанности Исполнителя:***

4.2.1 Предоставить Заказчику список участников Исполнителя, непосредственно оказывающих предусмотренные Договором услуги, а также документы, подтверждающие их квалификацию в соответствии с действующим законодательством.

4.2.2. Оказывать услуги по адресу Заказчика.

4.2.3. Оказывать услуги, в соответствии с техническими, санитарными, пожарными и иными требованиями.

4.2.4. Информировать Заказчика о ходе исполнения обязательств по Договору.

4.2.5. Немедленно письменно предупредить Заказчика при обнаружении не зависящих от Исполнителя обстоятельств, которые грозят годности результатов оказываемых услуг либо создают невозможность их оказания в установленный срок и/или в соответствии с иными условиями Договора.

4.2.6. При оказании услуг выполнять требования действующих нормативных документов по технике безопасности и охране окружающей среды.

4.2.7. Исполнять полученные в ходе оказания услуг указания Заказчика, устранять обнаруженные им недостатки или иные отступления от условий.

4.2.8. Не передавать техническую и иную документацию третьим лицам без письменного согласия Заказчика.

4.2.9. Оказывать услуги в надлежащие сроки.

4.2.10. Оказывать услуги в соответствии с требованиями Заказчика (Приложение № 1 к Договору).

4.2.11. Выполнить услуги в соответствии действующим законодательством, в сроки, установленные настоящим Договором.

4.2.12. Немедленно письменно предупредить Заказчика при обнаружении не зависящих от Исполнителя обстоятельств, которые грозят годности или прочности результатов выполняемых услуг либо создают невозможность их завершения в срок.

4.2.13. Исполнять полученные в ходе оказания услуг указания Заказчика, которые заносятся в соответствующие журналы, а также в срок, установленный предписанием Заказчика, устранять обнаруженные им недостатки в оказываемых услугах или иные отступления от условий настоящего Договора.

4.2.14. Гарантировать качество оказанных услуг не менее 12 месяцев с момента прекращения действия договора.

4.2.15. Своевременно устранять недостатки и дефекты, выявленные в результате оказанных услуг.

4.2.16. Выполнить иные обязанности, предусмотренные действующим законодательством и настоящим Договором.

 4.2.17. Нести риск случайного повреждения материалов (оборудования), используемого для оказания услуг или уничтожения их до момента сдачи результата оказания услуг Заказчику.

4.2.18. Представлять по запросу Заказчика в сроки, указанные в таком запросе, информацию о ходе исполнения обязательств по Договору.

4.2.19. Соблюдать конфиденциальность в отношении всей информации, ставшей известной Исполнителю в связи с исполнением обязательств по Договору.

4.2.20. Выполнить иные обязанности, предусмотренные действующим законодательством и настоящим Договором.

4.2.21. Исполнитель вправе требовать подписания документов об исполнении им обязательств по Договору от Заказчика.

4.2.22. Исполнитель вправе требовать оплаты по Договору в случае надлежащего исполнения своих обязательств по Договору.

**5. Качество услуг**

* 1. Гарантии качества распространяются на все услуги, оказанные Исполнителем по настоящему Договору.

5.2. Качество услуг оказываемых Исполнителем по настоящему Договору должно соответствовать требованиям государственных стандартов.

5.3. Гарантийный срок на оказанные услуги не менее 12 месяцев с момента прекращения действия договора

 5.4. Все данные в системе должны обрабатываться в соответствии с требованиями к защите информации от несанкционированного доступа. Информация должна предоставляться Пользователям в соответствии с их уровнем доступа, определенным Заказчиком.

5.5. Исполнитель обязан не передавать третьим лицам информацию, используемую для оказания услуг, и сведения о характере оказываемых услуг.

5.6. Исполнитель обязан оказывать услуги с соблюдением действующих правил и норм техники безопасности, пожарной безопасности, а также иных утвержденных и зарегистрированных в установленном порядке актов уполномоченных органов государственной власти в сфере охраны труда.

5.7. В процессе оказания услуг обработка и хранение персональных данных и конфиденциальной информации должны производиться в соответствии с действующим законодательством и организационно-распорядительными документами Заказчика.

5.8. Не допускается в процессе производства работ создание и/или применение отдельных (модульных, «оконных» и т.п.) систем, обслуживающих или взаимодействующих с МИС, разработанных сторонними правообладателями. Реализованные механизмы должны быть интегрированы в интерфейс МИС и корректно взаимодействовать с уже существующими функциональными механизмами.

5.9. Исполнитель обязан обеспечить работу МИС в составе внедренных сервисов и настроенной учетной политики.

5.10. Исполнитель обязан вносить изменения в аналитическую часть в соответствии с текущими требованиями Федеральных и региональных органов власти в рамках учета «Заболеваемости», «ВУТ», «посещаемости», «Диспансеризации и учета обслуживаемых контингентов».

5.11. Исполнитель обязан обеспечить программный продукт Заказчика обновлениями, выпускаемыми в промышленную эксплуатацию правообладателем программного продукта в срок не позднее чем 48 часов с момента выхода соответствующих обновлений (Клиентская и серверная части программного продукта).

Обновление МИС производится удаленно, путем размещения на сервере Заказчика пакетов обновления программных модулей и структуры хранилища данных МИС.

5.12. В случае модернизации, функциональные механизмы МИС не должны нарушать целостность существующих механизмов МИС, менять алгоритмы их работы, а также нарушать алгоритмы работы предприятия Заказчика без объективной необходимости.

5.13. Обеспечить Заказчика документом (Лицензионный договор или лицензионное соглашение с правообладателем программного продукта), подтверждающим право на использование обновленных версий (ревизий) МИС, устанавливаемых в связи с исполнением договора (приобретение неисключительных прав на объекты интеллектуальной собственности).

5.14. Поставку и инсталляцию обновлений МИС на оборудование Заказчика Исполнитель осуществляет самостоятельно.

5.15. Исполнитель обязан обеспечить возможность удаленного оперативного консультирования специалистов Заказчика по вопросам использования МИС следующими способами:

- по телефону горячей линии в рабочие дни с 09 до 17 часов;

- Интернет-служба (Онлайн) в виде возможности подачи электронных заявок с номерами заявок и возможностью отслеживания состояния и статусов заявок круглосуточно. При этом, Исполнитель обязан, по заявке заказчика, предоставить инструкцию по использованию такой службы, необходимые учетные записи для пользователей и т.п.

5.16. Исполнитель обязан устранить выявленные ошибки в работе МИС в сроки, указанные в Приложение № 1 к Договору.

**6. Порядок сдачи и приемки оказанных Услуг**

6.1. Заказчик осуществляет контроль за оказанием услуг, проверку соответствия объёма, срока и качества оказания услуг требованиям, установленным в Договоре.

6.2. При обнаружении Заказчиком в ходе приемки отдельных этапов или услуг по Договору в целом недостатков в оказанных услугах, Сторонами составляется акт, в котором фиксируется перечень недостатков и срок их устранения Исполнителем.

Исполнитель обязан устранить все обнаруженные недостатки своими силами и за свой счет в сроки, указанные в акте.

Устранение Исполнителем в установленные сроки выявленных Заказчиком недостатков не освобождает его от уплаты штрафных санкций, предусмотренных настоящим Договором.

6.3. По завершении в установленный срок услуг по Договору сторонами подписывается акт об оказании услуг.

6.4. Заказчик вправе отказаться от приемки результатов услуг в случае обнаружения недостатков, которые являются существенными и не могут быть устранены Исполнителем в сроки, согласованные с Заказчиком.

6.5. Оформлять первичные учетные документы и иные сопутствующие документы в форме электронных документов, подписанных усиленной квалифицированной электронной подписью (далее – электронные документы), включая, но не ограничиваясь следующими:

- на оказание услуг, а также отдельных этапов оказания услуг (далее - отдельный этап исполнения договора), включая все документы, предоставление которых предусмотрено в целях осуществления приемки оказанных услуг, а также отдельных этапов исполнения договора;

- результаты такой приемки;

- на оплату оказанных услуг, а также отдельных этапов исполнения договора.

6.6. Осуществлять обмен электронными документами с обязательным применением усиленной квалифицированной электронной подписи, для чего обеспечить получение Сторонами сертификатов ключа проверки электронной подписи в аккредитованном удостоверяющем центре в соответствии с нормами Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – КЭП). Осуществлять обмен электронными документами посредством системы электронного документооборота «СБИС Электронный документооборот» (далее – СБИС), для чего обеспечить в СБИС регистрацию лиц, уполномоченных за организацию и осуществление электронного документооборота.

6.7. При осуществлении обмена электронными документами использовать форматы документов, которые утверждены приказами ФНС России. Если форматы документов не утверждены, то Стороны используют согласованные между собой форматы.

6.8. Подписание электронного документа с помощью КЭП посредством СБИС означает, что документы и сведения, поданные в электронной форме:

- направлены от имени данных лиц,

- являются подлинными и достоверными,

- признаются равнозначными документам на бумажном носителе, подписанным собственноручной подписью.

6.9. Электронные документы, полученные Сторонами друг от друга при исполнении договора, не требуют дублирования документами, оформленными на бумажных носителях информации.

6.10. Электронный документ, подписанный КЭП, содержание которого соответствует требованиям нормативных правовых актов, должен приниматься Сторонами к учету в качестве первичного учетного документа, использоваться в качестве доказательства в судебных разбирательствах, предоставляться в государственные органы по запросам последних.

6.11. В случае невозможности обмена электронными документами при исполнении договора в связи с технической недоступностью СБИС Стороны обязаны информировать друг друга о невозможности обмена документами в электронном виде. В этом случае в период технической недоступности внутренних систем СБИС Стороны производят обмен документами на бумажном носителе с подписанием собственноручной подписью, при этом такая форма оригинала документа должна быть зафиксирована приказом руководителя направляющей Стороны.

После возобновления работы СБИС Сторона, ответственная за составление (оформление) документа, направляет с использованием СБИС Стороне, в адрес которой должен быть направлен соответствующий документ, сопроводительное письмо, подписанное КЭП уполномоченного лица, с приложением копии в электронной форме (скан-образа) документа, подписанного Сторонами на бумажном носителе информации.

Сторона, получившая в СБИС указанное сопроводительное письмо, осуществляет проверку сведений, содержащихся в сопроводительном письме и приложенной к нему копии в электронной форме (скан-образа) документа, на предмет их соответствия подписанному документу на бумажном носителе информации и по результатам проверки подписывает данное сопроводительное письмо КЭП уполномоченного лица либо аргументированно отказывается от его подписания.

**7. Ответственность Сторон**

7.1. В случае неисполнения или ненадлежащего исполнения своих обязательств по договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации и условиями договора.

7.2. В случае просрочки исполнения Заказчиком обязательств, предусмотренных договором, а также в иных случаях неисполнения или ненадлежащего исполнения Заказчиком обязательств, предусмотренных договором, Исполнитель вправе потребовать уплаты неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного договором, начиная со дня, следующего после дня истечения установленного договором срока исполнения обязательства. Такая пеня устанавливается в размере одной трехсотой действующей на дату уплаты пеней ключевой ставки Центрального банка Российской Федерации от не уплаченной в срок суммы.

7.3. В случае просрочки исполнения Исполнителем обязательств (в том числе гарантийного обязательства), предусмотренных договором, а также в иных случаях неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных договором, Заказчик вправе направить Исполнителю требование об уплате неустоек (штрафов, пеней).

7.4. Пеня начисляется за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного договором, начиная со дня, следующего после дня истечения установленного договором срока исполнения обязательства, и устанавливается в размере, определенном в соответствии с Правилами, но не менее чем одна трехсотая действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены договора, уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных договором и фактически исполненных Исполнителем.

7.5. Сторона освобождается от уплаты неустойки (штрафа, пени), если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного договором, произошло вследствие непреодолимой силы или по вине другой стороны.

Сторона, для которой в связи с названными обстоятельствами создалась невозможность выполнения своих обязательств по договору, в 3-дневный срок письменно извещает другую Сторону о невозможности выполнения обязательств по договору с указанием причин.

7.6. Все споры и разногласия разрешаются путем переговоров между Сторонами с обязательным составлением протокола переговоров, подписываемого представителями обеих Сторон. Если соглашение не достигнуто, то разрешение противоречий производится в претензионном порядке.

В случае если Стороны не придут к соглашению, споры подлежат рассмотрению в порядке, установленным действующим законодательством Российской Федерации, в Арбитражном суде Архангельской области.

**8. Срок действия Договора**

8.1. Договору вступает в силу с даты его подписания и действует до полного исполнения Сторонами принятых на себя обязательств по настоящему Договору либо до его расторжения.

8.2. Окончание срока действия настоящего Договора влечет за собой прекращение обязательств Сторон по нему, но не освобождает Стороны от ответственности за неисполнение или ненадлежащее исполнение Сторонами обязательств по настоящему Договору, если таковые имели место при исполнении настоящего Договора.

**9. Порядок изменения и расторжения Договора**

9.1. При заключении и исполнении Договора изменение его условий по соглашению Сторон и в одностороннем порядке не допускается, за исключением случаев, предусмотренных настоящим Договором.

9.2. Все изменения и дополнения к настоящему Договору действительны, если они оформлены в виде дополнительного соглашения к Договору и подписаны уполномоченными на то представителями Сторон. Дополнительные соглашения к Договору являются его неотъемлемой частью и вступают в силу с момента их подписания Сторонами.

9.3. При исполнении Договора не допускается перемена Исполнителя, за исключением случаев, если новый Исполнитель является правопреемником Исполнителя по настоящему Договору вследствие реорганизации юридического лица в форме преобразования, слияния или присоединения.

9.4. При изменении юридического адреса, банковских реквизитов, организационно-правовой формы Исполнитель в двухнедельный срок обязан письменно известить об этом Заказчика.

9.5. В случае перемены Заказчика по настоящему Договору права и обязанности Заказчика по данному Договору переходят к новому Заказчику в том же объеме и на тех же условиях.

9.6. Расторжение Договора допускается по соглашению Сторон, по решению суда, в случае одностороннего отказа Стороны Договора от исполнения Договора в соответствии с гражданским законодательством.

**10. Порядок разрешения споров**

10.1. Все споры и разногласия, возникшие в связи с исполнением настоящего Договора, Стороны будут стремиться решить путем переговоров, а достигнутые договоренности оформлять в виде дополнительных соглашений, подписанных представителями обеих Сторон и скрепленных печатями.

10.2. В случае недостижения взаимного согласия споры по настоящему Договору разрешаются в Арбитражном суде Архангельской области.

10.3. До передачи спора на разрешение Арбитражного суда Архангельской области Стороны примут меры к его урегулированию в претензионном порядке. Претензия должна быть направлена в письменном виде. По полученной претензии Сторона должна дать письменный ответ по существу в срок не позднее 5 рабочих дней с даты ее получения.

**11. Заключительные положения**

11.3. Взаимоотношения Сторон, не урегулированные настоящим Договором, регламентируются действующим законодательством Российской Федерации.

11.4. Неотъемлемыми частями Договора являются:

Приложение № 1 «Техническое задание».

Приложение № 2 «Спецификация».

**12. Адреса, реквизиты и подписи Сторон**

|  |  |
| --- | --- |
| **Заказчик:**165150, Архангельская обл., г. Вельск, ул. Дзержинского, д.42Телефон: (8-818-36) 6-42-74 Факс: (8-818-36) 6-43-82e-mail: gvsp@bk.ru gayzaovsp@yandex.ruБанковские реквизиты:ИНН 2907002500. КПП 290701001Министерство финансов Архангельской области (ГАУЗ АО «ВСП» л/сч 30246Э23710, 32246Э23710)Банк получателя: Р/счет 03224643110000002400 ОТДЕЛЕНИЕ АРХАНГЕЛЬСК БАНКА РОССИИ//УФК по Архангельской области и Ненецкому автономному округу г. АрхангельскБИК 011117401 Кор.счет 40102810045370000016 | **Исполнитель:** Адрес: ИНН КПП ОГРН Дата постановки на учет в налоговом органе: Обязательно заполняем: Обязательно прописать ОКОПФ, ОКПО, ОКТМО, ОКПФ+ электрон.почта Дата постановки на учет в налоговом органеМуниципальный район, городской округ, внутригородская территория в составе субъекта РФ **\***: Р/ сч. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_в\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_БИК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_К/сч. E-mail: Телефон:  |

 **Подписи сторон**

|  |  |  |
| --- | --- | --- |
| Главный врач ГАУЗ АО «ВСП» |  |  |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /**Л.Н. Шестакова**/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**\_\_\_\_\_\_\_\_\_\_\_\_\_/

Приложение № 1

к Договору № \_\_\_\_\_\_\_\_

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2023 года

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**1.1. Наименование объекта закупки:** Оказание услуг по поставке средств защиты информации

**1.2. Объем оказываемых услуг:**

|  |  |  |  |
| --- | --- | --- | --- |
| **№п/п** | **Наименование услуги** | **Ед. изм.** | **Количество** |
| 1 | Поставка средств защиты информации | Усл.ед. | 1 |

* 1. **Описание объекта закупки:**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Назначение продукта/модуля** | **Кол-во, шт.** |
| 1 | Средство защиты информации от несанкционированного доступа (далее – СЗИ от НСД) | СЗИ НСД должна представлять собой программный комплекс средств защиты информации в операционных системах (ОС) семейства Windows с возможностью подключения аппаратных идентификаторов.СЗИ НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 в многопользовательском режиме их эксплуатации.СЗИ НСД должна поддерживать 32- и 64-битные версии операционных систем.СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go.СЗИ НСД должна быть сертифицирована на соответствие требованиям руководящих документов к 5-му классу защищенности от НСД для СВТ (РД СВТ, Гостехкомиссия России, 1992) и 4-му уровню доверия («Требования по безопасности информации, устанавливающие уровни доверия к СТЗИ и СОБИТ», ФСТЭК России, 2020), разрабатываться и производиться на основании лицензии федеральных органов, имеющих полномочия в указанной сфере. Модуль СКН должен быть сертифицирован на соответствие требованиям ФСТЭК России к средствам контроля съемных машинных носителей информации по 4-му классу защиты в соответствии с профилем защиты средств контроля подключения съемных машинных носителей информации (ИТ.СКН.П4.ПЗ).СЗИ НСД может быть использована:* при создании защищенных автоматизированных систем до класса защищенности 1Г включительно;
* в государственных информационных системах до 1 класса защищенности включительно;
* в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно;
* в информационных системах персональных данных до 1 уровня защищенности включительно;
* при защите значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно.

СЗИ НСД должна обеспечивать:регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере. Возможность автоматического блокирования неактивных учетных записей пользователей;идентификацию и проверку подлинности пользователей при входе в ОС. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность задать расписание работы пользователей. Возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность аппаратного идентификатора конкретному пользователю. Возможность запрета повторного использования идентификатора. Возможность ограничения количества неуспешных попыток входа и блокирования устройства. Возможность автоматизированно сохранять авторизационные данные пользователя в системном кэше ОС при использовании (установке) СЗИ НСД. Поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows. Поддержку аутентификации пользователей с применением биометрии и токенов JaCarta PKI/BIO;реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам;возможность автоматического выбора аппаратного идентификатора в окне авторизации при входе в ОС;возможность настройки принудительной двухфакторной аутентификации для учетной записи с правами администратора и/или пользователя;возможность средствами СЗИ НСД выполнить настройку периода действия учетной записи;возможность настройки предупреждения пользователя до входа в систему о том, что в информационной системе реализованы меры по обеспечению безопасности информации;возможность при создании учетной записи выбрать тип учетной записи (внутренний, внешний, системный, приложение, гостевой, временный);независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), реестру, сети, съемным носителям информации. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных;контроль аппаратной конфигурации компьютера и следующих подключаемых устройств:* + Android-устройств;
	+ iOS-устройств;
	+ Bluetooth-устройств;
	+ DVD- и CD-ROM-дисководов;
	+ устройств HID, MTD, PCMCIA, IEEE 1394, Secure Digital;
	+ USB-контроллеров;
	+ беспроводных устройств (Wireless Communication Devices);
	+ биометрических устройств;
	+ дисководов магнитных дисков;
	+ звуковых, видео- и игровых устройств;
	+ инфракрасных устройств (IrDA);
	+ контроллеров магнитных дисков;
	+ ленточных накопителей;
	+ модемов;
	+ переносных устройств;
	+ портов (COM и LPT);
	+ сенсоров;
	+ сетевых адаптеров;
	+ сканеров и цифровых фотоаппаратов;
	+ принтеров;
	+ съемных носителей информации (CD-ROM, FDD, USB-Flash-накопителей).
* контроль устройств, подключаемых к терминальному серверу с RDP‑клиентов (контроль перенаправления устройств);
* предотвращение утечки информации с использованием съемных носителей информации. СЗИ НСД должна позволять разграничивать доступ как к отдельным типам носителей, так и к конкретным экземплярам;
* возможность запретить запуск (без команды пользователя) ПО, используемого для взаимодействия со съемными носителями информации;
* возможность запретить установку драйверов съемных носителей информации;
* преобразование информации:
* при работе с виртуальными дисками (преобразование выполняется незаметно для пользователя);
* при создании преобразованных файлов-контейнеров, используемых для хранения информации на внешних носителях или для передачи по различным каналам связи.

блокировку виртуальных дисков с преобразованной информацией при отключении аппаратного идентификатора;сохранение теневых копий файлов, записываемых на съемные носители;автоматическое ограничение доступа к теневой копии, сделанной СЗИ НСД при копировании документа, содержащего информацию ограниченного доступа, на сменный машинный носитель;использование дискреционного принципа контроля доступа, обеспечивающего доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа);возможность ограничивать средствами СЗИ НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа);регистрацию и учет (аудит) действий пользователей независимыми от ОС средствами (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки и автоматической архивации по истечении установленного интервала времени; расширенные возможности аудита печати: печать документов с возможностью добавления штампа (произвольного или по ГОСТ), возможность сохранения теневых копий распечатываемых документов, разграничение доступа пользователей к печати и нанесению штампов;возможность добавления произвольного комментария к зарегистрированным событиям НСД;возможность экспорта журналов событий в syslog, возможность настройки кодировки экспортируемых в syslog событий;возможность организации замкнутой программной среды (ЗПС) и различные способы ее настройки;блокировку доступа к файлам по расширению;возможность разграничения доступа к буферу обмена;возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов);возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений. Возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности;очистку остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Возможность определения метода зачистки. Контроль зачистки при полной зачистке логического диска. Очистку данных сеанса пользователя в оперативной памяти за счет запрета смены пользователя без перезагрузки;возможность проверки цифровой подписи объектов файловой системы, находящихся под контролем целостности, при их обновлении;выполнение регистрации действий по зачистке остаточной информации;самодиагностика основных функциональных возможностей СЗИ НСД и сохранение информации в виде отчета;возможность сохранения конфигурации для последующего восстановления СЗИ НСД; возможность настройки всех параметров СЗИ НСД из единой консоли администрирования;возможность создания отчета по назначенным правам, формирование паспорта программного обеспечения, установленного на ПЭВМ, формирование паспорта аппаратной части ПЭВМ;ведение двух копий программных средств защиты информации и возможность возврата к настройкам по умолчанию;возможность сигнализации администратору безопасности о следующих инцидентах безопасности (ситуациях сбоя функционирования и ситуациях несанкционированного доступа на клиентских рабочих станциях):* + нарушение контроля целостности объекта;
	+ попытка работы после блокировки при нарушении целостности;
	+ попытка входа на клиентскую рабочую станцию с неправильным паролем;
	+ блокировка пользователя после многократного ввода неправильного пароля;
	+ СЗИ НСД на клиенте не отвечает (возможная причина - несанкционированная деактивация системы защиты);
	+ клиент недоступен долгое время (с возможностью задания периода времени);
	+ попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами.

централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учетными записями пользователей, политиками, правами пользователей, преобразованными съемными носителями информации. Должна поддерживаться многоуровневая иерархия групп компьютеров и наследование установленных параметров. Также этим модулем должен осуществляться периодический сбор журналов со всех защищенных рабочих станций. Возможность блокировки компьютера, завершения сеанса работы пользователя по команде администратора;Должен быть реализован модуль контроля подключения съемных машинных носителей информации (СКН).Модуль СКН должен обеспечивать:контроль использования интерфейсов ввода/вывода средств вычислительной техники, подключения внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации;возможность назначения прав доступа к конкретному накопителю;возможность установить описание для сменного накопителя.Реализация СЗИ НСД должна быть полностью программной с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, а также аппаратных идентификаторов: * USB-флэш-накопители;
* электронные ключи Touch Memory (iButton);
* HID Proximity-карты;
* USB-ключи Aladdin eToken Pro/Java;
* смарт-карты Aladdin eToken Pro/SC;
* USB-ключи и смарт-карты Рутокен (Rutoken), Рутокен ЭЦП, Рутокен ЭЦП 2.0;
* USB-ключи и смарт-карты JaCarta, JaCarta-2, JaCarta PRO, JaCarta LT, JaCarta PKI/BIO;
* USB-ключи и смарт-карты ESMART;
* NFC-метки и смарт-карты семейства MIFARE.

Поставка СЗИ НСД должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием всех необходимых модулей и требуемого количества лицензий по каждому модулю. Варианты формулировок:* неисключительное право на использование СЗИ (НСД, СКН) (программное обеспечение)
 | 25 |
| 2 | Система антивирусной защиты | Программные средства Системы должны обеспечивать определение угроз следующих типов:* классических вирусов;
* троянских программ;
* руткитов;
* сетевых червей;
* рекламных программ;
* программ автодозвона на платные сайты;
* потенциально опасных приложений;
* прочих вредоносных программ.

Антивирусная защита должна обеспечивать:* обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п.;
* обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками;
* обнаружение вирусов внутри контейнеров и архивных файлов формата ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (включая NRG, образы с нестандартным форматом сектора и не имеющие сигнатур), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER с зашифрованными контейнерами и т.д. без ограничений на уровень вложенности проверяемых объектов;
* обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME);
* обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т.д.);
* антивирусную проверку файлов и объектов, имеющих формат Smart Install Maker (SIM); DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); INNO SETUP (5.3.9 и выше); SETUP FACTORY (линейки 7,8); XENOCODE; TARMA INSTALL (линейка 3); XZ (UNIX); COMPRESS; SQUAHFS; CHILKAT ZIP; пакеты LHA (AWARD BIOS);
* антивирусную проверку в самораспаковывающихся архивах: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy;
* проверку исполняемых файлов упакованных следующими упаковщиками: PELOCK, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, а также почтовых файлов Mozilla Thunderbird- вне зависимости от их размера;
* разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF;
* защиту от вредоносных программ, принадлежащих семействам вредоносных программ, информация о которых имеется в антивирусных базах, созданных после занесения соответствующей информации в антивирусные базы и еще не попавших на анализ в антивирусные лаборатории - как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;
* обнаружение вредоносных объектов в HTML- и PDF-документах, включая обфусцированные эксплойты в JavaScript, находящиеся в документах данных типов. Возможность извлечения и анализа «невидимых» IFRAME-элементов. Возможность извлечения для проверки скриптов любой сложности и снятие с них защиты;
* обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA);
* обнаружение угроз направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля

Используемое антивирусное ядро:* не должно допускать снижение скорости проверки при увеличении размера антивирусных баз;
* в связи с возможностью исчерпания ресурсов ОС (в том числе места на диске, памяти) в ходе обработки специальным образом сформированных архивов автоматически выбирать уровень анализа упакованных объектов, а также механизм уменьшения размера промежуточных файлов. При выборе уровня анализа должен учитываться уровень загрузки системы
* в целях ускорения проверки архивов и упакованных файлов должно обеспечивать опознание вредоносных программ без запуска распаковщика;
* должно обеспечивать защиту от так называемых «почтовых бомб»;
* должно обеспечивать работу с файлами размером как менее, так и больше 2 ГБ;
* должно поддерживать работу с дисками с LBA-адресацией;
* в целях исключения «утечки» оперативной памяти должно использовать механизм распределения динамической памяти уровня антивирусного ядра.

**Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows**Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:* осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях.

Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО, сертифицированного на соответствие требованиям к средствам антивирусной защиты (Приказ ФСТЭК России от 20.03.2012 г. № 28), должна обеспечивать защиту рабочих станций под управлением операционных систем:* + - * Microsoft Windows XP Professional;
			* Microsoft Windows 7;
			* Microsoft Windows 8.1;

Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур.Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов.Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках имеющихся у них прав.В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:* + - * поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
			* непрерывное фоновое сканирование в целях нейтрализации активных угроз
			* проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;
			* проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
			* блокировку опасных макросов VBA в реальном времени;
			* защиту от вредоносных сценариев, загружаемых с Web-страниц;
			* защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана;
			* проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО;
			* защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе отдельным типам сменных носителей информации, локальным файлам и каталогам, сайтам в сети Интернет;
			* ограничения доступа к сети Интернет или к компьютеру в определенный момент времени по расписанию
			* помещение найденных зараженных файлов в специальное место на жестком диске -«карантин»;
			* просмотр местоположения станций и серверов на карте, если заданы географические координаты станции
			* автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
			* запуск задач по расписанию и/или сразу после загрузки операционной системы;
			* возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке.

Система защиты рабочих станций должна обеспечивать проверку протоколов: * + - HTTP;
		- IMAP, SMTP, POP3 независимо от используемого почтового клиента;
		- NNTP (только проверка на вирусы), независимо от почтового клиента.

Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством:* + - антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
		- проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.

В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.Система должна обеспечивать защиту от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе шифровальщиков, а также блокировщиков экрана) с помощью превентивной защиты, отслеживающей попытки внедрения вредоносных файлов В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.**Требования по комплектности поставки**В состав Системы должны входить:* + - * программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания;
			* обновляемые базы данных сигнатур всевозможных вредоносных программ.

Комплект поставки должен содержать:* + - * необходимый набор серийных номеров либо ключевых файлов;
			* дистрибутив Системы;
			* файлы эксплуатационной документации в формате pdf (Adobe Acrobat Reader), в том числе руководство пользователя (администратора). Поставляемая документация должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

Комплект поставки, сертифицированный ФСТЭК России, должен содержать:* DVD-диск в фирменном конверте, содержащий верифицированные дистрибутивы сертифицированных продуктов
* документацию и материалы в формате PDF для настройки поставляемого программного обеспечения в соответствии с сертифицированными параметрами, приведенными в технической документации;
* формуляр, содержащий эталонные значения контрольных сумм сертифицированных продуктов;
* лицензионный сертификат, удостоверяющий законное приобретение программного изделия;
* заверенную копию сертификата соответствия ФСТЭК России.
 | 1 |
| 3 | Средство криптографической защиты информации (средство электронной подписи) | **Требования к реализации криптографических стандартов**Применяемое средство криптографической защиты информации (средство электронной подписи) должно обеспечивать применение электронной подписи (ЭП) и шифрования в соответствии с нормами действующего законодательства Российской Федерации и осуществлять выполнение следующих основных функций:* генерацию и управление ключевой информацией;
* формирование электронной подписи в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018) (в усиленном режиме формирование электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001 запрещено с 1 января 2020 года);
* подтверждение подлинности электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (ГОСТ 34.10-2012);
* подсчет значения хэш-функции в соответствии с ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018);
* шифрование и расшифрование данных в соответствии с ГОСТ 28147-89;
* формирование ключей электронной подписи и ключей проверки электронной подписи, а также ключей шифрования;
* идентификацию, аутентификацию, шифрование, имитозащиту TLS соединений;
* реализацию набора протоколов IPsec в соответствии с особенностями использования отечественных криптографических алгоритмов.

**Требования к реализации программного интерфейса встраивания**Средство криптографической защиты информации (средство электронной подписи) должно соответствовать криптографическому интерфейсу компании Microsoft - Cryptographic Service Provider (CSP).Встраивание средства криптографической защиты информации (средства электронной подписи) в прикладную информационную систему должно предусматривать возможность:* Применения в операционных системах семейства Microsoft Windows интерфейса функций:
* CAPICOM;
* Certificate Enrollment Control;
* Certificate Enrollment API;
* Certificate Services.
* вызова функций средства криптографической защиты информации (средства электронной подписи);
* применения в стандартном прикладном программном обеспечении операционных систем семейства Microsoft Windows MS Outlook Express; MS IE; MS IIS; Outlook, и т.д. (для поддержки MS Office Word, Excel может требоваться дополнительное ПО от разработчика средства криптографической защиты информации (средства электронной подписи)).

**Требования к алгоритмам, сертификатам открытых ключей и поддерживаемым форматам криптографических сообщений**Применяемое средство криптографической защиты информации (средство электронной подписи) должно реализовывать ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Информационная технология. Криптографическая защита информации. Блочные шифры», ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018) «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».Применяемое средство криптографической защиты информации (средство электронной подписи) должно реализовывать ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 и ГОСТ 28147-89 с учетом RFC 4357 «Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms», ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 34.10-2018, ГОСТ 34.10-2018. Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать сертификаты открытых ключей стандарта X.509v3 согласно RFC 5280 «Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile» с учетом RFC 4491 «Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile», а также документа Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), «Техническая спецификация. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509».Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать формат криптографических сообщений согласно RFC 3852 «Cryptographic Message Syntax (CMS)» с учетом RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)», а также документа Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS».Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать возможность создания форматов криптографических сообщений типа CAdES в соответствии с ETSI TS 101 733 (Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)): * формата CAdES-BES;
* формата CAdES–T;
* формата СAdES-X Long Type 1,

а также формата XML DSign для формирования электронной подписи в XML при встраивании в прикладные информационные системы с использованием программных библиотек (SDK) от разработчика средства криптографической защиты информации (средства электронной подписи). Отдельные компоненты таких программных библиотек могут лицензироваться дополнительно.**Требования к составу**Комплектация исполнения средства криптографической защиты информации (средства электронной подписи) должна включать:* Модуль сетевой аутентификации TLS, обеспечивающий реализацию сетевого протокола TLS с использованием российских криптографических стандартов (возможности модуля TLS определяются типом лицензии на средство криптографической защиты информации (средство электронной подписи))

**Функциональные требования**Средство криптографической защиты информации (средство электронной подписи) должно предоставлять программный интерфейс для выполнения следующих основных функций:* формирование электронной подписи на рабочем месте пользователя;
* подтверждение подлинности электронной подписи на серверах и рабочих местах пользователей;
* подсчет значения хэш-функции данных на серверах и рабочих местах пользователей;
* шифрование и расшифрование данных на рабочем месте пользователя и (или) сервере (в зависимости от типа лицензии);
* формирование ключей электронной подписи и ключей проверки электронной подписи на рабочем месте пользователя и (или) сервере (в зависимости от типа лицензии);
* поддержка аппаратных средств визуализации подписываемой информации, включая форматы подписи таких аппаратных устройств (типа Рутокен PinPad)

Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать выполнение следующих сервисных функций:* встраивание средства криптографической защиты информации в прикладную информационную систему должно предусматривать возможность использования библиотеки SDK TLS в мобильные приложения без проведения исследований по оценке влияния ОС мобильных устройств на СКЗИ.
* установка личных сертификатов и ключей проверки электронной подписи на рабочем месте/сервере с обеспечением связи сертификата открытого ключа с соответствующим указанному сертификату закрытым ключом;
* копирование и удаление ключей электронной подписи;
* установка, изменение и удаление пароля на доступ к закрытому ключу.
* создание и проверка электронной подписи в формате CMS (присоединенной и отсоединенной) с использованием графического интерфейса пользователя;
* Установка параметров работы в режиме «Облачного провайдера», включая определение сетевых адресов подключения, установку сертификатов ключей проверки электронной подписи, хранящихся в «облачном токене».

Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать эксплуатацию на следующих операционных системах (иметь клиентскую лицензию):* Windows 7/8/8.1/10 (x86/x64).

**Требования к сертификации** Средство электронной подписи (средство криптографической защиты информации) должно быть сертифицировано или иметь положительное Заключение ФСБ России по требованиям:* К средствам электронной подписи;
* К средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, по классам КС1, КС2, КС3.

Классы защиты КС2, КС3 могут обеспечиваться с учетом доступности ОС для конкретного класса защиты.Класс защиты КС3 должен обеспечиваться для функционирования СКЗИ в среде следующих операционных систем:Windows 7/8/8.1/10/Server 2008 (x86, x64);Windows Server 2008 R2/2012/2012 R2/2016 (x64). | 25 |

Страна происхождения – Россия

**2. Условия оказания услуг:**

2.1. Лицензия должна давать право:

- на использование программы на всей территории Российской Федерации.

- на использование программы на любом из языков, на котором она была издана Правообладателем.

**3. Требования к гарантийным обязательствам (требования к гарантии качества услуг, а также требования к гарантийному сроку и (или) объему предоставления гарантий ее качества):** Гарантийный срок на результат оказанных услуг, в рамках которого Исполнитель гарантирует Заказчику качественную бесперебойную работу Специализированного ПО без каких–либо функциональных ограничений, должен соответствовать сроку действия предоставленной лицензии, начиная с даты ее активации.

**4. Требования к качеству оказываемых услуг:**

Качество оказываемых услуг должно соответствовать условиям Контракта и требованиям государственных стандартов, технических норм и иных нормативных актов, установленных для данного вида услуг.

В случае оказания услуг, качество которых не соответствует условиям Контракта, Исполнитель без промедления обязуется устранить недостатки. Убытки, возникшие в связи с устранением недостатков, несет Исполнитель.

 **5. Передача неисключительных прав:** в рамках данной закупки предусмотрена.

|  |  |  |
| --- | --- | --- |
| Главный врач ГАУЗ АО «ВСП» |  |  |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /**Л.Н. Шестакова**/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**\_\_\_\_\_\_\_\_\_\_\_\_\_/

Приложение № 1

к техническому заданию

**«Сведения о местах оказания услуг»**

| **№ п/п** | **Наименование места оказания услуг** | **Адрес** | **Ф.И.О. контактного лица** | **Телефон** |
| --- | --- | --- | --- | --- |
| 1 | Государственное автономное учреждение здравоохранения Архангельской области «Вельская стоматологическая поликлиника»  | 165150, Архангельская обл., г. Вельск, ул. Дзержинского, д.42 | Зимарев Сергей Александрович | 8-818-36-64466 |

|  |  |  |
| --- | --- | --- |
| Главный врач ГАУЗ АО «ВСП» |  |  |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /**Л.Н. Шестакова**/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**\_\_\_\_\_\_\_\_\_\_\_\_\_/

Приложение № 2

к техническому заданию

**«Описание системы»**

1. **Полное наименование эксплуатируемой МИС:**

«Медицинская Информационная Система «Комплекс Программных Средств «Система Автоматизации Медико-Страхового Обслуживания Населения» «САМСОН»\*

1. **Назначение:**
	1. Данная система предназначена для автоматизации процессов управления лечебным учреждением
2. **Техническое описание эксплуатируемой МИС (ревизия 29727):**
	1. Серверная часть МИС:
		1. Система управления базами данных (СУБД): Сервер баз данных MariaDB – поддержка модели ACID, поддержка репликации данных, открытый исходный код, отсутствие требований дополнительного лицензирования, поддержка соединений с использованием ODBC, JDBC и .NET, поддержка стандарта ANSI/ISOSQL.
		2. Данные МИС хранятся и обрабатываются (добавление, изменение, удаление, запрос) путем обращения клиента к СУБД, указанной в п.3.1.1.
		3. Операционная система: Альт Сервер
		4. Интерфейс: командный интерпретатор bash
		5. Доступ к серверу БД: протокол TCP/IP
		6. Технология работы комплекса: клиент-сервер
		7. Безопасность: уровень операционной системы и СУБД
		8. Резервное копирование: ежедневное, автоматическое, по расписанию.
	2. «Клиентская» часть МИС:
		1. Интерфейс – графический (GUI)
		2. Реализация –с использованием «толстого» (Rich-) клиента.
		3. Инструментальная среда – Python, QT (не требует дополнительного лицензирования)
		4. Операционная среда: возможность работы под Альт рабочая станция, а также Windows 7 и выше.
		5. Почтовый клиент – встроенный (протокол SMTP/POP3)
		6. Безопасность: ролевой доступ на уровне клиентского интерфейса.
		7. Экспорт/Импорт – DBF, XML, SQL, HTML.
		8. Справочная система, использует международные и общероссийские классификаторы:
			1. МКБ Х
			2. ОКВЭД
			3. ОКПО
			4. ОКАТО
			5. ОКПФ
			6. ОКФС
			7. ОКСО
			8. КЛАДР
			9. РЛС
			10. МКС
		9. Система тарификации – поддерживает следующие типы финансирования:
			1. Бюджетное
			2. ДМС
			3. ОМС
			4. Платное
			5. Целевое
		10. Финансовый контроль – обеспечивает ведение договоров на предоставляемые услуги и выполняет мониторинг оплаты по оказанным услугам.
		11. Как серверная, так и клиентская часть МИС предусматривают возможность полноценной работы без использования программного обеспечения (в том числе операционной системы) требующего дополнительного лицензирования.
3. **На сервере МИС «САМСОН»\*, настроено автоматическое создание резервных копий баз данных, которые хранятся на жестких дисках сервера.**
	1. Для обеспечения надежности и возможности оперативного восстановления данных в случае выхода из строя сервера МИС «САМСОН», Заказчик обязан предоставить ресурс для дублирования резервных копий баз данных в локальной сети учреждения, доступный с сервера МИС «САМСОН» в ночное время, по любому из следующих протоколов: SMB, FTP или SSH.
	2. Заказчик самостоятельно принимает решение о месте хранения, его объемах и условиях хранения данной информации.
	3. Исполнитель не несет ответственности за хранение этих данных.
	4. Запрещен свободный (без пароля) доступ к данному ресурсу. Объем, занимаемый резервными копиями, зависит от размера баз данных, а также от количества хранимых копий. Рекомендуемый объем – 100 Гб, минимальный – 10 Гб.

|  |  |  |
| --- | --- | --- |
| Главный врач ГАУЗ АО «ВСП» |  | Генеральный директор ООО «САМСОН Групп» |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /**Л.Н. Шестакова**/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**В.Н. Когаленок/

Приложение № 2

к Договору № 2581

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2023 года

**СПЕЦИФИКАЦИЯ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Наименование услуги** | **Единица измерения** | **Цена за единицу,****рублей** | **Кол-во единиц** | **Итого, рублей** |
| 1 | Предоставление простого (неисключительного) права на получение обновлений, эксплуатируемого программного продукта «Медицинская Информационная Система «Комплекс Программных Средств «Система Автоматизации Медико-Страхового Обслуживания Населения» «САМСОН» | Условная единица | 54 051,30 | 12 | 648 615,60 |
| 2 | Услуга по сопровождению и технической поддержке программного продукта «Медицинская Информационная Система «Комплекс Программных Средств «Система Автоматизации Медико-Страхового Обслуживания Населения» «САМСОН» | Условная единица | 6 005,70 | 12 | 72 068,40 |

ИТОГО: 720 684 рубля 00 копеек (семьсот двадцать тысяч шестьсот восемьдесят четыре рубля 00 копеек), НДС не облагается (п. 2 ст. 346.14 гл. 26.2 Налогового кодекса Российской Федерации).

|  |  |  |
| --- | --- | --- |
| Главный врач ГАУЗ АО «ВСП» |  | Генеральный директор ООО «САМСОН Групп» |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /**Л.Н. Шестакова**/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**В.Н. Когаленок/

|  |  |
| --- | --- |
|  | **Требование к содержанию, составу заявки на участие в электронном аукционе и к иным документам, предоставляемых оператором электронной площадки:** |
| 1 | **Предложение участника закупки в отношении объекта закупки:** |
| 1.1 | **характеристики предлагаемого участником закупки товара, соответствующие показателям***Примечание: Указание в описании на все товарные знаки в описании объекта закупки (в приложении к извещению) задании следует читать со словами «или эквивалент».* | Установлено, Приложение №1 – Описание объекта закупки |
| 1.2 | **наименование страны происхождения товара в соответствии с общероссийским классификатором, используемым для идентификации стран мира** | Установлено |
| 1.3 | **документы, подтверждающие соответствие товара, работы или услуги требованиям, установленным в соответствии с законодательством Российской Федерации** | Не установлено |
| 1.4 | **иные информация и документы, в том числе эскиз, рисунок, чертеж, фотография, иное изображение предлагаемого участником закупки товара. При этом отсутствие таких информации и документов не является основанием для отклонения заявки на участие в закупке** | Не установлено |
| 1.5 | **предложение участника закупки о цене контракта** | Не установлено |
| 1.6 | **предложение участника закупки о сумме цен единиц товара, работы, услуги** | Не установлено |
| 1.7 | **информация и документы, предусмотренные нормативными правовыми актами, принятыми в соответствии с частями 3 и 4 статьи 14 Федерального закона Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд» (с последующими изменениями), или копии этих документов.** *В случае отсутствия таких информации и документов в заявке на участие в закупке такая заявка приравнивается к заявке, в которой содержится предложение о поставке товаров, происходящих из иностранного государства или группы иностранных государств, работ, услуг, соответственно выполняемых, оказываемых иностранными лицами.* | подтверждением происхождения программ для электронных вычислительных машин и баз данных из Российской Федерации является наличие в реестре российского программного обеспечения сведений о таких программах для электронных вычислительных машин и баз данных;подтверждением, что программа для электронных вычислительных машин и баз данных относится к государству - члену Евразийского экономического союза, за исключением Российской Федерации, является наличие в реестре евразийского программного обеспечения сведений о таких программах для электронных вычислительных машин и баз данных. |
| 2 | **Информация и документы об участнике закупки** |
| 2 | **Для юридических лиц** *(не включаются в заявку на участие в закупку, но направляются (по состоянию на дату и время их направления) оператором электронной площадки, путем информационного взаимодействия с единой информационной системой)* | * полное и сокращенное (при наличии) наименование юридического лица, в том числе иностранного юридического лица (если участником закупки является юридическое лицо), аккредитованного филиала или представительства иностранного юридического лица (если от имени иностранного юридического лица выступает аккредитованный филиал или представительство), наименование обособленного подразделения юридического лица (если от имени участника закупки выступает обособленное подразделение юридического лица);
* фамилия, имя, отчество (при наличии), идентификационный номер налогоплательщика (при наличии) и должность лица, имеющего право без доверенности действовать от имени юридического лица, либо действующего в качестве руководителя юридического лица, аккредитованного филиала или представительства иностранного юридического лица, либо исполняющего функции единоличного исполнительного органа юридического лица;
* идентификационный номер налогоплательщика (при наличии) или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика таких лиц следующих лиц:
1. идентификационный номер налогоплательщика (при наличии);
2. членов коллегиального исполнительного органа;
3. лица, исполняющего функции единоличного исполнительного органа, управляющего (при наличии),
4. управляющей организации (при наличии),
5. участников (членов) корпоративного юридического лица, владеющих более чем двадцатью пятью процентами акций (долей, паев) корпоративного юридического лица,

 учредителей унитарного юридического лица;* адрес юридического лица, в том числе иностранного юридического лица (если участником закупки является юридическое лицо) в пределах места нахождения юридического лица, адрес (место нахождения) аккредитованного филиала или представительства на территории Российской Федерации (если от имени иностранного юридического лица выступает аккредитованный филиал или представительство), адрес (место нахождения) обособленного подразделения юридического лица (если от имени участника закупки выступает обособленное подразделение юридического лица);
* адрес электронной почты;
* номер контактного телефона;
* идентификационный номер налогоплательщика юридического лица (если участником закупки является юридическое лицо), аккредитованного филиала или представительства иностранного юридического лица (если от имени иностранного юридического лица выступает аккредитованный филиал или представительство);
* код причины постановки на учет юридического лица, аккредитованного филиала или представительства иностранного юридического лица (если от имени иностранного юридического лица выступает аккредитованный филиал или представительство), обособленного подразделения юридического лица (если от имени участника закупки выступает обособленное подразделение юридического лица);
* выписка из единого государственного реестра юридических лиц;
* надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица в соответствии с законодательством соответствующего государства (если участником закупки является иностранное лицо);
* реквизиты счета участника закупки, на который в соответствии с законодательством Российской Федерации осуществляется перечисление денежных средств в качестве оплаты поставленного товара, выполненной работы (ее результатов), оказанной услуги, а также отдельных этапов исполнения контракта, за исключением случаев, если в соответствии с законодательством Российской Федерации такой счет открывается после заключения контракта;
 |
| 2.2 | **Для физических лиц, зарегистрированных в качестве индивидуального предпринимателя** *(не включаются в заявку на участие в закупку, но направляются (по состоянию на дату и время их направления) оператором электронной площадки, оператором путем информационного взаимодействия с единой информационной системой)* | * фамилия, имя, отчество (при наличии);
* место жительства физического лица;
* адрес электронной почты;
* номер контактного телефона;
* идентификационный номер налогоплательщика физического лица, аналог идентификационного номера налогоплательщика в соответствии с законодательством соответствующего иностранного государства (если участником закупки является иностранное лицо)
* выписка из единого государственного реестра индивидуальных предпринимателей;
* надлежащим образом заверенный перевод на русский язык документов о государственной регистрации физического лица в качестве индивидуального предпринимателя в соответствии с законодательством соответствующего государства (если участником закупки является иностранное лицо);
* реквизиты счета участника закупки, на который в соответствии с законодательством Российской Федерации осуществляется перечисление денежных средств в качестве оплаты поставленного товара, выполненной работы (ее результатов), оказанной услуги, а также отдельных этапов исполнения контракта, за исключением случаев, если в соответствии с законодательством Российской Федерации такой счет открывается после заключения контракта
 |
| 2.3 | **Для физических лиц не зарегистрированных в качестве индивидуального предпринимателя** *(не включаются в заявку на участие в закупку, но направляются (по состоянию на дату и время их направления) оператором электронной площадки, путем информационного взаимодействия с единой информационной системой)* | * фамилия, имя, отчество (при наличии);
* копия документа, удостоверяющего личность участника закупки в соответствии с законодательством Российской Федерации;
* место жительства физического лица;
* адрес электронной почты;
* номер контактного телефона;
* идентификационный номер налогоплательщика физического лица, аналог идентификационного номера налогоплательщика в соответствии с законодательством соответствующего иностранного государства (если участником закупки является иностранное лицо)

реквизиты счета участника закупки, на который в соответствии с законодательством Российской Федерации осуществляется перечисление денежных средств в качестве оплаты поставленного товара, выполненной работы (ее результатов), оказанной услуги, а также отдельных этапов исполнения контракта, за исключением случаев, если в соответствии с законодательством Российской Федерации такой счет открывается после заключения контракта; |
| 2.4 | **декларация о принадлежности участника закупки к учреждению или предприятию уголовно-исполнительной системы** *(не включаются в заявку на участие в закупку, но направляются (по состоянию на дату и время их направления) оператором электронной площадки, путем информационного взаимодействия с единой информационной системой)* | Не установлено |
| 2.5 | **декларация о принадлежности участника закупки к организации инвалидов, предусмотренной частью 2 статьи 29 Федерального закона № 44-ФЗ от 05.04.2013 (если участник закупки является такой организацией)***(не включаются в заявку на участие в закупку, но направляются (по состоянию на дату и время их направления) оператором электронной площадки, путем информационного взаимодействия с единой информационной системой)* | Не установлено |
| 2.6 | **декларация о принадлежности участника закупки к социально ориентированным некоммерческим организациям в случае установления преимущества, предусмотренного частью 3 статьи 30 Федерального закона № 44-ФЗ от 05.04.2013 года***(не включаются в заявку на участие в закупку, но направляются (по состоянию на дату и время их направления) оператором электронной площадки, путем информационного взаимодействия с единой информационной системой)* | Установлено |
| 2.7 | документы, подтверждающие соответствие участника такого аукциона требованиям, установленным пунктом 1 части 1 статьи 31 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд» (с последующими изменениями), или копии этих документов | Не установлено |
| 2.8 | **документы, подтверждающие соответствие участника такого аукциона требованиям, установленным части 2 статьи 31 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд» (с последующими изменениями), или копии этих документов***(не включаются в заявку на участие в закупке и направляются (по состоянию на дату и время их направления) оператором электронной площадки из реестра участников закупок, аккредитованных на электронной площадке)* | Не установлено |
| 2.9 | **документы, подтверждающие соответствие участника такого аукциона требованиям, установленным части 2.1 статьи 31 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд» (с последующими изменениями), или копии этих документов***(не включаются в заявку на участие в закупке и направляются (по состоянию на дату и время их направления) оператором электронной площадки из реестра участников закупок, аккредитованных на электронной площадке)* | Не установлено |
| 2.10 | **декларация о соответствии участника закупки требованиям, установленным пунктами 3 - 5, 7 - 11 части 1 статьи 31 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд» (с последующими изменениями)** | Необходимо предоставить в составе заявки |
| 2.11 | **решение о согласии на совершение или о последующем одобрении крупной сделки, если требование о наличии такого решения установлено законодательством Российской Федерации, учредительными документами юридического лица и для участника закупки заключение контракта на поставку товара, выполнение работы или оказание услуги, являющихся объектом закупки, либо внесение денежных средств в качестве обеспечения заявки на участие в закупке, обеспечения исполнения контракта является крупной сделкой** | Необходимо предоставить в составе заявки, за исключением участников – физических лиц, в том числе зарегистрированных в качестве индивидуального предпринимателя |

В соответствии с частью 3 статьи 27 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд» участники закупки имеют право выступать в отношениях, связанных с осуществлением закупки, как непосредственно, так и через своих представителей. Полномочия представителей участников закупки подтверждаются доверенностью, выданной и оформленной в соответствии с гражданским законодательством.

**ИНСТРУКЦИЯ ПО ЗАПОЛНЕНИЮ ЗАЯВКИ НА УЧАСТИЕ В ЭЛЕКТРОННОМ АУКЦИОНЕ**

**Для участия в закупке необходимо подать заявку на участие, которая должна содержать документы и сведения, предусмотренные статьей 43 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд», с учетом требований настоящего извещения.**

При формировании предложения участника закупки в отношении объекта закупки:

1) информация о товаре, предусмотренная подпунктами "а" и "б" пункта 2 части 1 статьи 43 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд», включается в заявку на участие в закупке в случае осуществления закупки товара, в том числе поставляемого заказчику при выполнении закупаемых работ, оказании закупаемых услуг. Информация, предусмотренная подпунктом "а" пункта 2 части 1 статьи 43 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд», может не включаться в заявку на участие в закупке в случае указания заказчиком в описании объекта закупки товарного знака и предложения участником закупки товара, в том числе поставляемого заказчику при выполнении закупаемых работ, оказании закупаемых услуг, обозначенного таким товарным знаком;

2) информация, предусмотренная подпунктами "а" и "г" пункта 2 части 1 статьи 43 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд», не включается в заявку на участие в закупке в случае включения заказчиком в соответствии с пунктом 8 части 1 статьи 33 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд» в описание объекта закупки проектной документации, или типовой проектной документации, или сметы на капитальный ремонт объекта капитального строительства.

При формировании заявки на участие в закупке на поставку товаров, участники закупки предоставляют информацию о предлагаемом к поставке товаре в следующем порядке:

1) в случае установления в описании объекта закупки соответствующего минимального значения показателя товара с использованием слов/словосочетаний/символов «не менее…», «не ниже…», «не хуже…», «не уже…», «≥», «от…» участник закупки в заявке обязан указать конкретное значение показателя, не менее установленного в описании объекта закупки минимального значения показателя товара без использования указанных слов/словосочетаний/символов.

2) в случае установления в описании объекта закупки соответствующего максимального значения показателя товара с использованием слов/словосочетаний/символов «не более…», «не выше…», «не превышает…», «не должен превышать…», «не шире…», «до…», «≤», «не ранее…» участник закупки в заявке обязан указать конкретное значение показателя, не превышающее установленного в описании объекта закупки максимального значения показателя товара без использования указанных слов/словосочетаний/символов.

3) в случае установления в описании объекта закупки соответствующего минимального значения показателя товара с использованием слов/словосочетаний/символов «более…», «выше…», «свыше…», «больше…», «лучше…», «превосходит…», «должен превосходить…», «шире…», «>» участник закупки в заявке обязан указать конкретное значение показателя, превышающее установленное в описании объекта закупки минимальное значение показателя товара без использования указанных слов/словосочетаний/символов.

4) в случае установления в описании объекта закупки соответствующего максимального значения показателя товара с использованием слов/словосочетаний/символов «менее…», «ниже…», «меньше…», «уже…», «<»,«ранее…» участник закупки в заявке обязан указать конкретное значение показателя, меньшее по значению установленного в описании объекта закупки максимального значения показателя товара без использования указанных слов/словосочетаний/символов.

5) в случае установления в описании объекта закупки соответствующего минимального и максимального значения показателя товара, выражаемого как диапазон значений (требование к нижней и верхней границе диапазона значений), участник закупки в заявке обязан указать диапазон конкретных значений показателя товара (нижнюю и верхнюю границу диапазона значений), удовлетворяющий соответственно требованиям к минимальному и максимальному значению диапазона значений с учетом положений пунктов 1-4 настоящей Инструкции.

6) в случае установления требования к значению показателя в описании объекта закупки с применением слов/знаков «или», «либо», «/» участник закупки в заявке обязан указать одно из альтернативных значений показателя, а в случае использования «и/или» - одно или несколько значений через запятую.

7) в случае установления в описании объекта закупки нескольких значений показателя товара, перечисленных через «,» («…, …, …»), участник закупки в заявке обязан указать все перечисленные значения показателя, соответствующие установленным в описании объекта закупки требованиям к значению показателя товара.

8) в случае установления в описании объекта закупки соответствующего значения показателя товара, для которого указаны допустимые минимальное и максимальное значения, с использованием слов/словосочетаний «более … менее…», «не менее … менее…», «более … не более…», «не менее … не более…», «не ниже … не выше…», «выше … не выше…», «выше … ниже…», «не ниже … ниже…», «менее… более…», «не более… более…», «менее… не менее…», «не более… не менее…», «ниже… выше…», «не выше… выше…», «ниже… не ниже…», «не выше… не ниже…», «более … и менее…», «не менее … и менее…», «более … и не более…», «не менее … и не более…», «не ниже … и не выше…», «выше … и не выше…», «выше … и ниже…», «не ниже … и ниже…», «менее… и более…», «не более… и более…», «менее… и не менее…», «не более… и не менее…», «ниже… и выше…», «не выше… и выше…», «ниже… и не ниже…», «не выше… и не ниже…», «не уже… не шире…», «шире …. не шире…», «не уже… уже…», «шире… уже…», «±», «ранее… и не ранее …» участник закупки должен указать конкретное значение показателя, соответствующее установленным Заказчиком требованиям без использования указанных слов/словосочетаний с учетом положений пунктов 1-4 настоящей Инструкции.

9) При установлении в описании объекта закупки требований к одному показателю в разных единицах измерения, участник закупки вправе указать все или выбрать одну из представленных единиц измерения, в иных случаях участник закупки в своей заявке обязан указать все единицы измерения, установленные заказчиком.

10) Все сведения, содержащиеся в заявке участника закупки, не должны допускать двусмысленных толкований. В значениях показателей предложения участника не должно содержать слов: «или эквивалент», «или», «должен» (и его производные), «и/или», «либо», а также рекомендуется использовать общепринятые обозначения и наименования в соответствии с требованиями действующих нормативных документов для того, чтобы заказчик имел возможность оценить предложение участника на соответствие требованиям, указанным в описании объекта закупки.