областное государственное автономное учреждение здравоохранения
"Ангарская городская больница № 1"

Юридический адрес: 665830, Иркутская область, г. Ангарск, ул. Горького, 24
Почтовый адрес: 665806, Иркутская область, г. Ангарск, а/я 606

т. (3955) 52-37-87 эл. почта: ang_gb1@bk.ru ИНН: 3801012780 ОГРН: 1033800519191
ф. (3955) 52-32-97 сайт: angarsk-gb1.ru КПП: 380101001 ОКПО: 05248348

ПРОТОКОЛ РАССМОТРЕНИЯ И ОЦЕНКИ ЗАЯВОК НА УЧАСТИЕ В ЗАПРОСЕ КОТИРОВОК В ЭЛЕКТРОННОЙ ФОРМЕ № 862

«21» ноября 2017

Запрос котировок в электронной форме проводится в соответствии с Положением о закупках товаров, работ, услуг для нужд областного государственного автономного учреждения здравоохранения «Ангарская городская больница № 1», утвержденным протоколом наблюдательного совета ОГАУЗ «Ангарская городская больница № 1» от 15.09.2017г. № 07-2017 (далее - Положение).

Закупка	31705733822 от 14.11.2017
Наименование закупки:	Предоставление не исключительных прав использования антивирусных программных продуктов
Способ проведения закупки:	Запрос котировок в электронной форме
Наименование электронной площадки в сети Интернет	OTC-tender
Адрес электронной площадки в сети Интернет	tender.otc.ru
Заказчик	
Наименование организации:	областное государственное автономное учреждение здравоохранения «Ангарская городская больница № 1»
Место нахождения:	665830, Иркутская область, г. Ангарск, ул. Горького, дом 24
Почтовый адрес:	665806, Иркутская область, г. Ангарск, а/я 606
Проведение процедуры	
Дата и время проведения процедуры рассмотрения и оценки котировочных заявок:	21.11.2017г. 11:00
Место проведения процедуры рассмотрения и оценки котировочных заявок:	г. Ангарск, ул. Горького, дом 24, кабинет 419, 4 этаж
Дата подписания протокола:	21.11.2017

Сведения о комиссии:

На процедуре заседания Единой комиссии (далее - комиссии) по рассмотрению заявок на участие в запросе котировок в электронной форме присутствуют:

Ф.И.О.	Должность	Статус
Председатель комиссии:		
И.В. Крывовязый	Главный врач ОГАУЗ «Ангарская городская больница № 1»	присутствует
Члены комиссии:		
Д.И. Гончарук	Заместитель главного врача по ФЭР ОГАУЗ «Ангарская городская больница № 1»	присутствует
М.М. Дубинина	И.о.главного бухгалтера ОГАУЗ «Ангарская городская больница № 1»	присутствует
Е.А. Маслакова	Юрисконсульт ОГАУЗ «Ангарская городская больница № 1»	присутствует
П.А. Жуков	Начальник отдела ИТ ОГАУЗ «Ангарская городская больница № 1»	присутствует
Секретарь комиссии:		
И.П. Пушница	Ведущий экономист ОГАУЗ «Ангарская городская больница № 1»	присутствует

Всего на заседании присутствовало 6 членов конкурсной комиссии.

Кворум
Комиссия

имеется	V	не имеется	
правомочна	V	неправомочна	

Предмет договора
Предмет договора — Предоставление не исключительных прав использования антивирусных программных продуктов

Начальная (максимальная) цена договора: 40 740 (сорок тысяч семьсот сорок) рублей 00 копеек, включая НДС

Срок поставки товара, выполнения работ, оказания услуг — с 01.01.2018 по 31.12.2018

Место поставки товара, выполнения работ, оказания услуг: — г. Ангарск, ул. Горького, дом 24

Сведения о наименовании и объеме закупаемых товаров работ, услуг:

п/п	Наименование Услуг	Характеристика Услуг	Ед. изм.	Количество	Начально-максимальная цена услуги, руб.
1	Dr.Web Desktop Security Suite (Комплексная Защита) + ЦУ, на 12 месяцев, 200 ПК EDU/MED Продление	**Общие характеристики:** Все компоненты принадлежат одной торговой марке с единой службой технической поддержки на русском языке. Срок действия лицензии не менее 12 месяцев с момента передачи Заказчику.	шт.	1	36190,00
2	Антивирус Dr.Web Server Security Suite + ЦУ, на 12 месяцев, 2 ПК EDU/MED Продление	В рамках всей организации используются единые антивирусные средства независимо от степени конфиденциальности обрабатываемой информации. Отдельно стоящие ПК, то есть не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, защищены интегрированным программным продуктом, включающим в себя защиту от всех типов вредоносных программ (антивирус), спама (персональный антиспам) и обеспечивают возможность их включения в единую систему антивирусной защиты. Программный интерфейс всех антивирусных средств, включая средства управления на русском языке. Все антивирусные средства, функционирующие под операционной системой типа Windows, включая средства управления, обладают контекстной справочной системой на русском языке. Лицензионные ключевые файлы имеют возможность отложенной активации, и срок их действия начинается с момента установки. **Характеристики программных средств антивирусной защиты рабочих станций и серверов под управлением ОС семейства Microsoft Windows** Программные средства Системы обеспечивают реализацию следующих функциональных возможностей: осуществление антивирусной защиты на серверах, выполняющих функции серверов терминалов и принт-серверов, серверов приложений и контроллеров доменов, файловых серверов. Осуществление антивирусной и антиспам защиты на рабочих станциях. Программные средства Системы обеспечивают определение в объектах файловой системы сервера угроз следующих типов: классических вирусов, сетевых червей,	шт.	1	4550,00

		троянских программ, программ-реклам, потенциально опасных приложений, прочих вредоносных программ. Программное обеспечение, используя актуальную на момент проведения тендера версию, обеспечивает защиту рабочих станций под управлением операционных систем: Microsoft XP Professional (Service Pack 2 и выше) и Home Edition, Microsoft Vista и Windows Seven. Система, используя актуальную на момент проведения тендера версию, обеспечивает защиту для файловых серверов под управлением операционных систем Microsoft 2003 Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003 все Service Packs, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition, Microsoft 2008 Server. Компоненты Системы устойчиво функционирует на серверах и рабочих станциях класса Pentium III в условиях их минимальной и максимальной загрузки без существенного снижения производительности серверов. Компоненты системы имеют 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 поставляется в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, с электронной почтой, с локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Система построена по клиент-серверной архитектуре с возможностью построения иерархической системы серверов как на основе ОС Microsoft Windows, так и на основе ОС типа UNIX (Linux, FreeBSD, Solaris). Система имеет возможность использования как внешней, так и внутренней СУБД. При использовании внешней СУБД Система имеет возможность работы с ней как напрямую (с СУБД PostgreSQL, MS SQL, Oracle), так и через драйвера ODBC. Система имеет возможность замены типа используемой СУБД после установки серверной части по требованию Администратора. Программные средства управления для всех защищаемых ресурсов, реализованных на платформах ОС Microsoft Windows обеспечивают реализацию следующих функциональных возможностей: построение многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне; централизованная удаленная установка и деинсталляция программных средств, антивирусных баз и антивирусного ядра на рабочие станции и сервера Windows; выбор и настройка устанавливаемых компонентов до начала установки антивирусного пакета на клиентские части; централизованное обновление антивирусных баз на всех защищенных рабочих станциях и серверах, в том числе мобильных и находящихся в режиме off-line; доставка обновлений на рабочие места пользователей как по расписанию, так сразу после их получения; обновление программных средств и антивирусных баз из разных источников, как по каналам			

		связи, так и на машинных носителях информации; автоматический переход установленного ПО на более новые версии, в том числе с возможностью выбора обновляемых компонентов; централизованный сбор статистической информации и создание отчетов о состоянии антивирусной защиты и их консолидация; наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий); отправка информационных сообщений пользователям по сети в режиме реального времени через консоль Системы и Web-интерфейс; самостоятельное написание обработчиков событий. Система обладает специальной политикой для мобильных пользователей (ноутбуки) при применении которой мобильные пользователи должны иметь возможность редактирования настроек антивирусного пакета и обновления через Интернет при отсутствии доступа к антивирусному серверу. Применение политики должно происходить как из стандартной консоли администратора Системы, так и через Web-интерфейс, без использования файлов конфигурации типа *.xml. Антивирусное программное обеспечение по умолчанию имеет оптимальные с точки зрения безопасности и производительности работы настройки. При этом в случае необходимости внесения изменений, Система обеспечивает возможность простого и гибкого изменения настроек пользователями и администраторами Системы в рамках, имеющихся у них прав. В Системе реализована возможность обеспечения связи антивирусного сервера и клиентских частей через встроенный модуль в случае, когда они расположены в различных сетях, работающих по протоколам TCP/IP/IPv6/IPX/NetBIOS, между которыми отсутствует маршрутизация пакетов. В случае реализации иерархической системы серверов, Система автоматически перераспределяет рабочие станции для получения обновлений между серверами в целях снижения общей нагрузки на сеть. Система обладает возможностью автоматического поиска и деинсталляции сторонних средств антивирусной защиты перед установкой антивирусного пакета на клиентские рабочие станции и сервера. Система поддерживает возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции и сервера сети без их предварительного лечения с последующим лечением системы. Система обладает возможностью встроенного автоматического резервного копирования критически важных данных и конфигурации антивирусного сервера по заранее заданному расписанию, а также опцию восстановления сервера из резервной копии без использования файлов конфигурации типа *.xml. Права доступа к настройкам компонентов антивирусного пакета для пользователей определяются администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля. Система имеет возможность управления защитой сети с			

		помощью консоли администратора, которая может быть установлена на любой компьютер в сети и иметь возможность инсталяции на ОС Windows, ОС семейства Unix, MacOS. Система имеет возможность удаленного администрирования с помощью Web-интерфейса через любой Web-браузер. Администратор Системы, не дожидаясь окончания процесса сканирования рабочих станций на наличие вредоносных кодов, имеет возможность в режиме реального времени осуществлять контроль за ходом процесса сканирования на любой рабочей станции. Система имеет возможность автоматического мониторинга трафика антивирусной сети. Система имеет возможность интеграции с платформой Microsoft® Network Access Protection (NAP), обеспечивающей автоматическую систему реагирования на инциденты безопасности. Система имеет журнал аудита действий администраторов Системы, позволяющий просматривать журнал событий и изменений, осуществленных администраторами при помощи консоли. В Системе реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов. Система имеет возможность централизованной настройки параметров защиты, уникальных для различных групп, в том числе для рабочих станций, находящихся в режиме off-line. Система имеет возможность выбора уровня подробности протоколирования обмена информацией между своими компонентами. Система обеспечивает проверку любых объектов на защищаемых рабочих станциях и серверах, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора. Система обеспечивает на рабочих станциях и серверах поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера; 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 архивных файлов формата ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR т.д. без ограничений на уровень вложенности проверяемых объектов; 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; защиту от еще неизвестных вредоносных программ, принадлежащих зарегистрированным семействам, как на основе эвристического анализа, так и с помощью дополнительных технологий. 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; блокировку опасных макросов VBA в реальном времени; защиту от программ автодозвона на платные сайты, вредоносных сценариев, загружаемых с Web-страниц; помещение найденных зараженных файлов в специальное место на жестком диске - «карантин»; автоматический запуск антивирусного программного обеспечения и других необходимых компонент 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 под управлением семейства ОС Microsoft Windows обеспечивает реализацию следующих функциональных возможностей: защиту входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама. Обеспечивается обнаружение и удаление вирусов всех типов, как из тела сообщения, так и вложенных файлов. Осуществляется проверка трафика на следующих протоколах: защиту HTTP-трафика - проверку всех объектов, поступающих на компьютер пользователя по протоколу HTTP, FTP только на уровне Internet шлюзов, защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа локальным и сетевым ресурсам. В том числе сменным дискам, каталогам и сайтам Интернет. Система защиты рабочих станций обеспечивает проверку протоколов: IMAP, SMTP, POP3, независимо от используемого почтового клиента; NNTP (только проверка на вирусы), независимо от почтового клиента. Система обеспечивает 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 по команде пользователя или администратора и по расписанию, заключающегося в однократной полной или выборочной проверке на наличие угроз объектов; проверки на лету с помощью антивирусной резидентной программы объектов при доступе к ним. В Системе 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 работает на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы. В Системе реализована защита работы собственных модулей от сбоев и случайного изменения. Система обладает возможностью задания групповых политик в зависимости от группы IP-адресов. В Системе, не имеющей доступа к сети Интернет, реализована возможность обновления вирусных баз путём скачивания их с сервера разработчика Системы с возможностью последующего их переноса в Систему с помощью любого носителя информации. Система обеспечивает реализацию следующих функциональных возможностей по обновлению: система получает ежедневные обновления вирусных баз не менее			

		10 раз в сутки независимо от того, рабочий, либо выходной день, что должно подтверждаться созданным Системой отчетом (лог-файлом), система поддерживает множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации, система обладает функцией автоматической докачки обновлений антивирусных компонентов и вирусных баз на серверной части в случае обрыва связи с Интернетом в процессе обновления. Система поддерживает проверку целостности и подлинности обновлений средствами электронной цифровой подписи. Система имеет возможность шифрования трафика между серверами и рабочими станциями в целях предотвращения утечки конфиденциальной информации. Система имеет сертификат соответствия ФСБ России требованиям к антивирусным средствам класса А1с. Система сертифицирована уполномоченным органом (ФСТЭК) на соответствие ТУ и НДВ 4 на применение в составе подсистемы антивирусной защиты информационных системах персональных данных (ИСПДн) класса К1. Система сертифицирована уполномоченным органом (ФСТЭК) на соответствие требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню контроля не ниже 4 и требованиям технических условий. **Комплектность:** В состав Системы входят: программные средства антивирусной защиты рабочих станций и серверов; программные средства централизованного управления, мониторинга и обновления; обновляемые базы данных сигнатур всевозможных вредоносных программ. **Техническая поддержка Системы:** Техническая поддержка предоставляется на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет. Web-сайт производителя Системы на русском языке, имеет специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов производителя.			

Котировочные заявки

Все заявки, предоставленные для участия в запросе котировок в электронной форме, были зарегистрированы в Журнале регистрации поступления котировочных заявок в порядке их поступления (Приложение № 1 к настоящему протоколу, являющееся неотъемлемой частью данного протокола). К сроку окончания подачи котировочных заявок была предоставлено 2(два) заявки.

Код участник	Наименование участника закупки	ИНН/КПП/ОГРН	Почтовый адрес	Цена договора, предложенная участником

а				закупки, руб.
1	Общество с ограниченной ответственностью Региональный сервисный центр "Форус"	3811123658 / 381101001 / 1083811006608	664007, Российская Федерация, Иркутская обл., г. Иркутск, ул. Партизанская, 49	28 518,00 руб., НДС не облагается
2	ООО 'МастерСофт-ИТ'	5609061055 / 560901001 / 1065658007360	460052, Российская Федерация, Оренбургская обл., г. Оренбург, Монтажников, 26/2	40 740,00 руб., НДС не облагается

Решение комиссии

Единая комиссия рассмотрела заявки в соответствии с требованиями и условиями, установленными в извещении о проведении запроса котировок, и приняла следующие решения:

Код участника	Наименование (для юридического лица), фамилия, имя, отчество (для физического лица) участника размещения заказа	Решение комиссии
1	Общество с ограниченной ответственностью Региональный сервисный центр "Форус"	Допустить к участию в запросе котировок в электронной форме
2	ООО 'МастерСофт-ИТ'	Допустить к участию в запросе котировок в электронной форме

Результаты проведения запроса котировок в электронной форме

Единая комиссия решила заключить договор на предоставление не исключительных прав использования антивирусных программных продуктов с ООО РСЦ "Форус", с суммой договора 28 518 (двадцать восемь тысяч пятьсот восемнадцать) рублей 00 копеек, НДС не облагается, так как заявка участника закупки отвечает всем требованиям, установленным в извещении и документации запроса котировок в электронной форме.

Настоящий протокол подписан всеми присутствующими на заседании членами комиссии и подлежит направлению оператору электронной площадки и размещению на сайте www.zakupki.gov.ru.

Председатель комиссии:

Главный врач _____ И. В. Крывовязый

Члены комиссии:

Заместитель главного врача по ФЭР _____ Д.И. Гончарук

И.о.главного бухгалтера _____ М.М. Дубинина

Юрисконсульт _____ Е.А. Маслакова

Начальник отдела ИТ _____ П.А. Жуков

Секретарь комиссии:

Ведущий экономист _____ И.П. Пушница

Приложение № 1 к Протоколу рассмотрения и оценки заявок на участие в запросе котировок в электронной форме № 862 от 21.11.2017г.

ЖУРНАЛ РЕГИСТРАЦИИ ПОСТУПЛЕНИЯ КОТИРОВОЧНЫХ ЗАЯВОК

№ п/п	Входящий номер заявки	Дата поступления	Время поступления (время московское)	Код участника	Форма подачи заявки
1	661995	20.11.2017	11:13	1	электронная
2	662177	20.11.2017	15:09	2	электронная