Управление Федеральной антимонопольной службы

по республике Коми

РЕШЕНИЕ

09 августа 2016 года 04-02/7349

г. Сыктывкар

Комиссия Управления Федеральной антимонопольной службы по Республике Коми по контролю в сфере <……..> (далее - Комиссия Коми УФАС России), рассмотрев жалобу общества с ограниченной ответственностью «СИСТЕМЫ ПЛЮС» (далее - ООО «СИСТЕМЫ ПЛЮС», заявитель) исх. от 01.08.2016 (вх. от 02.05.2016 № 2368э) на действия аукционной комиссии заказчика – Государственного бюджетного учреждения здравоохранения Республики Коми «Городская больница Эжвинского района г. Сыктывкара» (далее – ГБУЗ РК «ГБЭР»), по факту принятия решения об отказе заявителю в допуске к участию в электронном аукционе, объектом которого является «Поставка антивирусного программного обеспечения», извещение № 307200008716000200 (далее - закупка, электронный аукцион, жалоба),

при участии:

<……..>,

<……..>,

УСТАНОВИЛА:

1. ООО «СИСТЕМЫ ПЛЮС», ГБУЗ РК «ГБЭР», закрытое акционерное общество «Сбербанк - Автоматизированная система торгов» (далее - ЗАО «Сбербанк - АСТ») надлежащим образом о времени и месте рассмотрения жалобы извещены посредством электронной почты.

Письмом исх. от 03.08.2016 (вх. от 03.08.2016 №2391э.), ООО «СИСТЕМЫ ПЛЮС» было заявлено ходатайство о рассмотрении жалобы в отсутствие их представителя.

С учетом законодательно установленных сроков рассмотрения жалобы отсутствие представителей ООО «СИСТЕМЫ ПЛЮС», ЗАО «Сбербанк - АСТ» не препятствует рассмотрению жалобы по существу.

2. ООО «СИСТЕМЫ ПЛЮС» обжалованы действия аукционной комиссии заказчика в части отказа в допуске его заявки к участию в аукционе, причиной отказа

послужило следующее:

- сведения, содержащиеся в первой части заявки на участие в электронном аукционе, не соответствуют требованиям, установленным п/п 1б) ч. 3 п. 12 и п/п 1 ч.3 п.14 раздела I; пункта 27 раздела II; раздела III (Техническое задание) документации об электронном аукционе, а именно не представлены конкретные показатели предлагаемого для поставки товара, установленные документацией об аукционе:

ГБУЗ РК «ГБЭР» в отзыве на жалобу исх. от 08.08.2016 №2180/1 (вх. № 08.08.2016 №4034), и на заседании Комиссии Коми УФАС России заявлены возражения относительно позиции заявителя.

3. Комиссия Коми УФАС России в ходе проведения внеплановой проверки осуществления закупки в соответствии с пунктом 1 части 15 статьи 99 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее - Закон о контрактной системе), изучив материалы жалобы, заслушав представителей ГБУЗ РК «ГБЭР», пришла к нижеследующим выводам.

Заказчиком закупки путем проведения электронного аукциона явилось Государственное бюджетное учреждение здравоохранения Республики Коми «Городская больница Эжвинского района г. Сыктывкара».

Объект закупки - «Поставка антивирусного программного обеспечения».

Начальная (максимальная) цена договора составила 47 050.00 рублей.

Источником финансирования закупки явились средства бюджетного учреждения за счет средств ОМС.

Извещение о проведении электронного аукциона № 0307200008716000200, документация электронного аукциона размещены на официальном сайте Единой информационной системе в сфере закупок 15.07.2016.

4. Согласно части 1 статьи 59 Закона о контрактной системе под аукционом в электронной форме (электронным аукционом) понимается аукцион, при котором информация о закупке сообщается заказчиком неограниченному кругу лиц путем размещения в единой информационной системе извещения о проведении такого аукциона и документации о нем, к участникам закупки предъявляются единые требования и дополнительные требования, проведение такого аукциона обеспечивается на электронной площадке ее оператором.

Согласно пункту 1 части 1 статьи 64 Закона о контрактной системе документация об электронном аукционе наряду с информацией, указанной в извещении о проведении такого аукциона, должна содержать наряду с прочей информацией наименование и описание объекта закупки и условия контракта в соответствии со статьей 33 настоящего Федерального закона, в том числе обоснование начальной (максимальной) цены контракта.

В соответствии с частью 1 статьей 33 Закона о контрактной системе заказчик при описании в документации о закупке объекта закупки должен руководствоваться следующими правилами:

- описание объекта закупки должно носить объективный характер. В описании объекта закупки указываются функциональные, технические и качественные характеристики, эксплуатационные характеристики объекта закупки (при необходимости). В описание объекта закупки не должны включаться требования или указания в отношении товарных знаков, знаков обслуживания, фирменных наименований, патентов, полезных моделей, промышленных образцов, наименование места происхождения товара или наименование производителя, а также требования к товарам, информации, работам, услугам при условии, что такие требования влекут за собой ограничение количества участников закупки, за исключением случаев, если не имеется другого способа, обеспечивающего более точное и четкое описание характеристик объекта закупки. Документация о закупке может содержать указание на товарные знаки в случае, если при выполнении работ, оказании услуг предполагается использовать товары, поставки которых не являются предметом контракта. При этом обязательным условием является включение в описание объекта закупки слов "или эквивалент", за исключением случаев несовместимости товаров, на которых размещаются другие товарные знаки, и необходимости обеспечения взаимодействия таких товаров с товарами, используемыми заказчиком, а также случаев закупок запасных частей и расходных материалов к машинам и оборудованию, используемым заказчиком, в соответствии с технической документацией на указанные машины и оборудование;

- использование при составлении описания объекта закупки показателей, требований, условных обозначений и терминологии, касающихся технических характеристик, функциональных характеристик (потребительских свойств) товара, работы, услуги и качественных характеристик объекта закупки, которые предусмотрены техническими регламентами, принятыми в соответствии с законодательством Российской Федерации о техническом регулировании, документами, разрабатываемыми и применяемыми в национальной системе стандартизации, принятыми в соответствии с законодательством Российской Федерации о стандартизации, иных требований, связанных с определением соответствия поставляемого товара, выполняемой работы, оказываемой услуги потребностям заказчика. Если заказчиком при составлении описания объекта закупки не используются установленные в соответствии с законодательством Российской Федерации о техническом регулировании, законодательством Российской Федерации о стандартизации показатели, требования, условные обозначения и терминология, в документации о закупке должно содержаться обоснование необходимости использования других показателей, требований, условных обозначений и терминологии;

- описание объекта закупки может включать в себя спецификации, планы, чертежи, эскизы, фотографии, результаты работы, тестирования, требования, в том числе в отношении проведения испытаний, методов испытаний, упаковки в соответствии с требованиями Гражданского кодекса Российской Федерации, маркировки, этикеток, подтверждения соответствия, процессов и методов производства в соответствии с требованиями технических регламентов, документов, разрабатываемых и применяемых в национальной системе стандартизации, технических условий, а также в отношении условных обозначений и терминологии;

- документация о закупке должна содержать изображение поставляемого товара, позволяющее его идентифицировать и подготовить заявку, окончательное предложение, если в такой документации содержится требование о соответствии

поставляемого товара изображению товара, на поставку которого заключается контракт;

- документация о закупке должна содержать информацию о месте, датах начала и окончания, порядке и графике осмотра участниками закупки образца или макета товара, на поставку которого заключается контракт, если в такой документации содержится требование о соответствии поставляемого товара образцу или макету товара, на поставку которого заключается контракт;

- документация о закупке должна содержать указание на международные непатентованные наименования лекарственных средств или при отсутствии таких наименований химические, группировочные наименования, если объектом закупки являются лекарственные средства. Заказчик при осуществлении закупки лекарственных средств, входящих в перечень лекарственных средств, закупка которых осуществляется в соответствии с их торговыми наименованиями, а также при осуществлении закупки лекарственных препаратов в соответствии с пунктом 7 части 2 статьи 83 настоящего Федерального закона вправе указывать торговые наименования этих лекарственных средств. Указанный перечень и порядок его формирования утверждаются Правительством Российской Федерации. В случае, если объектом закупки являются лекарственные средства, предметом одного контракта (одного лота) не могут быть лекарственные средства с различными международными непатентованными наименованиями или при отсутствии таких наименований с химическими, группировочными наименованиями при условии, что начальная (максимальная) цена контракта (цена лота) превышает предельное значение, установленное Правительством Российской Федерации, а также лекарственные средства с международными непатентованными наименованиями (при отсутствии таких наименований с химическими, группировочными наименованиями) и торговыми наименованиями;

- поставляемый товар должен быть новым товаром (товаром, который не был в употреблении, в ремонте, в том числе который не был восстановлен, у которого не была осуществлена замена составных частей, не были восстановлены потребительские свойства) в случае, если иное не предусмотрено описанием объекта закупки.

Раздел III «Наименование и описание объекта закупки (Техническое задание)» документации об электронном аукционе (далее - Техническое задание) содержит следующую информацию:

№ п/п	Наименование товара	Характеристики товара (в том числе: форма предоставления)	Срок действия	Ед. изм.	Кол-во
1	2	3	4	5	6
1	Антивирусное программное обеспечение (неисключительное право)	Базовая. Форма предоставления – лицензия. На русском языке	1 год	шт	50
		Средства антивирусной			

№ п/п	Наименование товара	Характеристики товара (в том числе: форма предоставления)	Срок действия	Ед. изм.	Кол-во
		средства анализа) или защиты предназначенные для развертывания в государственных организациях должны быть			
2	Дистрибутив	сертифицированы 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 2 и требованиям технических условий. Специальный сертифицированный медиа-пак должен состоять из: - лицензионный продукт с записанными сертифицированными приложениями; -формуляр-документа, подтверждающего, что данный лицензионный продукт действительно содержит сертифицированные приложения; - заверенных копий сертификатов	бессрочно	шт	1

Технические требования к программным средствам антивирусной защиты.

Общие требования:

Антивирусные средства включают:

- Программные средства антивирусной защиты для рабочих станций Windows.
- Программные средства антивирусной защиты для рабочих станций Linux.
- Программные средства антивирусной защиты для файловых серверов Windows.
- Программные средства антивирусной защиты для файловых серверов Linux.

• Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows.

• Программные средства антивирусной защиты для мобильных устройств (смартфонов).

• Программные средства централизованного управления, мониторинга и обновления.

• Обновляемые базы данных сигнатур вредоносных программ и атак.

• Эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления-на русском языке.

Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке.

Требования к программным средствам антивирусной защиты для рабочих станций Windows

Программные средства антивирусной защиты для рабочих станций Windows функционируют на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows 2000 Professional (Service Pack 4 Rollup1)
- Microsoft Windows Vista Business / Enterprise / Ultimate SP1 и выше
- Microsoft Windows Vista Business / Enterprise / Ultimate x64 Edition SP1 и выше
- Microsoft Windows XP Professional SP2 и выше
- Microsoft Windows XP Professional x64 Edition SP2
- Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate SP0 и выше
- Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate x64 Edition SP0 и выше
- Microsoft Windows 8 Professional / Enterprise
- Microsoft Windows 8 Professional / Enterprise x64 Edition
- Microsoft Windows Embedded Standard 7 SP1
- Microsoft Windows Embedded Standard 7 x64 Edition SP1
- Microsoft Windows Embedded POS Ready 2009

Программные средства антивирусной защиты для рабочих станций Windows обеспечивают реализацию следующих функциональных возможностей:

- Резидентный антивирусный мониторинг.

- Программные средства защиты от сетевых атак.

- Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.

- Обнаружение скрытых процессов.

- Антивирусное сканирование по команде пользователя или администратора и по расписанию.

- Антивирусная проверка и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.

- Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем.

- Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу.

- Защита электронной корреспонденции, как от вредоносных программ, так и от спама, с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 — независимо от используемого почтового клиента; независимо от типа протокола (в том числе MAPI, HTTP) — в рамках работы плагинов, встроенных в почтовые программы Microsoft Office Outlook и TheBat!.

- Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP.

- Проверка скриптов — проверка скриптов, обрабатываемых в Microsoft Internet Explorer, а также WSH-скриптов (таких как JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в интернете.

- Проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет-пейджерами.

- Запуск задач по расписанию или сразу после загрузки операционной системы.

- Защита от еще не известных вредоносных программ на основе анализа их поведения и контроля изменений системного реестра, с возможностью автоматического восстановления изменённых вредоносной программой значений системного реестра.

- Автоматический контроль программ, запускаемых на компьютере пользователя, осуществляющий контроль активности программ и ограничивающий выполнение опасных действий.

- Защита от хакерских атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные.

- Проверка протокола IPv6.

- Защита от программ-маскировщиков, программ автодозвона на платные сайты.

- Блокировка баннеров, всплывающих окон, вредоносных сценариев, загружаемых с Web-страниц.

- Распознавание и блокировка фишинг-сайтов.

• Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и запуск программ. Компонент должен контролировать приложения по пути нахождения программы, метаданным, контрольной сумме MD5.

• Осуществление контроля работы пользователя с внешними устройствами ввода/вывода, позволяя ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям.

• Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.

• Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

• Интеграция с системой обновления Windows Update для установки патчей, закрывающих обнаруженные уязвимости.

• Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.

- Настройка проверки критических областей компьютера в виде отдельной задачи.

• Технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющие избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.

• Возможность установки только выбранных компонентов программного средства антивирусной защиты.

- Централизованное управление с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для рабочих станций Mac

Программные средства антивирусной защиты для рабочих станций Mac

функционируют на компьютерах, работающих под управлением операционных систем следующих версий:

- Mac OS X 10.4.11 и выше.

Программные средства антивирусной защиты для рабочих станций Mac обеспечивают реализацию следующих функциональных возможностей:

• Резидентный антивирусный мониторинг.

• Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.

• Антивирусное сканирование по команде пользователя или администратора и по расписанию.

• Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.

• Централизованно управляться с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для рабочих станций Linux

Программные средства антивирусной защиты для рабочих станций Linux функционируют на компьютерах, работающих под управлением операционных систем следующих версий:

32-битные платформы:

- Red Hat Enterprise Linux 5.8 Desktop
- Red Hat Enterprise Linux 6.2 Desktop
- Fedora 16
- CentOS-6.2
- SUSE Linux Enterprise Desktop 10 SP4
- SUSE Linux Enterprise Desktop 11 SP2
- openSUSE Linux 12.1
- openSUSE Linux 12.2
- Debian GNU/Linux 6.0.5
- Mandriva Linux 2011
- Ubuntu 10.04 LTS
- Ubuntu 12.04 LTS

64-битные платформы:

- Red Hat Enterprise Linux 5.8 Desktop
- Red Hat Enterprise Linux 6.2 Desktop
- Fedora 16
- CentOS-6.2
- SUSE Linux Enterprise Desktop 10 SP4
- SUSE Linux Enterprise Desktop 11 SP2
- openSUSE Linux 12.1
- openSUSE Linux 12.2
- Debian GNU/Linux 6.0.5
- Ubuntu 10.04 LTS
- Ubuntu 12.04 LTS

Программные средства антивирусной защиты для рабочих станций Linux обеспечивают реализацию следующих функциональных возможностей:

- Резидентный антивирусный мониторинг.
- Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.
- Антивирусное сканирование по команде пользователя или администратора и по расписанию.
- Антивирусная проверку и лечение файлов в архивах.
- Запуск задач по расписанию и/или сразу после загрузки операционной системы.
- Помещение подозрительных и поврежденных объектов на карантин.
- Возможность экспортировать и сохранять отчеты в форматах HTML и CSV.
- Возможность перехвата и проверки файловых операций на уровне SAMBA.
- Гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
- Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность.
- Возможность управления через графический интерфейс.
- Централизованно управляться с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Windows

Программные средства антивирусной защиты для файловых серверов Windows функционируют на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows 2000 Server/Advanced Server (Service Pack 4 Rollup1)
- Microsoft Windows Server 2003 Standard/Enterprise (Service Pack 2)
- Microsoft Windows Server 2003 x64 Standard/Enterprise (Service Pack 2)
- Microsoft Windows Server 2003 R2 Standard/Enterprise Edition (Service Pack 2)
- Microsoft Windows Server 2003 R2 x64 Standard/Enterprise Edition (Service Pack 2)
- Microsoft Windows Small Business Server 2003 R2 (Service Pack 2)
- Microsoft Windows Server 2008 Standard/Enterprise (Service Pack 1 или выше)
- Microsoft Windows Server 2008 x64 Standard/Enterprise (Service Pack 1 или выше)
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2008 Standard x64 Edition
- Microsoft Windows Essential Business Server 2008 Standard / Premium
- Microsoft Windows Server 2008 R2 x64 Standard/Enterprise SP0 и выше
- Microsoft Windows Server 2008 Foundation Edition
- Microsoft Windows Server 2008 R2 Foundation x64 Edition SP0 и выше
- Microsoft Windows MultiPoint Server 2010
- Microsoft Windows MultiPoint Server 2011 x64 edition
- Microsoft Small Business Server 2011 Essentials / Standard / Premium x64 Edition
- Microsoft Windows Server 2012 Foundation x64 Edition (без поддержки ReFS и режима Core)
- Microsoft Windows Server 2012 Essentials x64 Edition (без поддержки ReFS и режима Core)
- Microsoft Windows Server 2012 Standard x64 Edition (без поддержки ReFS и режима Core)

Терминальныесервисы:

- Terminal Services (Remote Desktop Services) набазе Windows Server 2008 R2.

Программные средства антивирусной защиты для файловых серверов Windows

обеспечивают реализацию следующих функциональных возможностей:

- Резидентный антивирусный мониторинг.

- Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.

- Программные средства защиты от сетевых атак.

- Защита от хакерских атак, путем использования межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа.

- Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу.

- Обнаружение скрытых процессов.

- Антивирусное сканирование по команде пользователя или администратора и по расписанию.

- Антивирусная проверка и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.

- Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем.

- Запуск задач по расписанию и/или сразу после загрузки операционной системы.

- Защита от еще не известных вредоносных программ, принадлежащих зарегистрированным семействам, на основе эвристического анализа.

- Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.

- Настройки проверки критических областей сервера в качестве отдельной задачи.

- Регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме.

- Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий).

- Технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, защиты файлов приложения от несанкционированного доступа и изменения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющими избежать отключения защиты со стороны вредоносных программ, злоумышленников или

неквалифицированных пользователей.

- Централизованное управление с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Mac OS

Программные средства антивирусной защиты для файловых серверов Mac OS функционирут на компьютерах, работающих под управлением операционных систем следующих версий:

- Mac OS X Server 10.6, 10.7

Программные средства антивирусной защиты для файловых серверов Mac OS обеспечивают реализацию следующих функциональных возможностей:

• Резидентный антивирусный мониторинг.

• Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.

• Антивирусное сканирование по команде пользователя или администратора и по расписанию.

• Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.

• Централизованно управляться с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Linux

Программные средства антивирусной защиты для файловых серверов Linux функционируют на компьютерах, работающих под управлением операционных систем следующих версий:

32-битные платформы:

- Red Hat Enterprise Linux 6.2 Server
- Red Hat Enterprise Linux 5.8 Server
- Fedora 16
- CentOS-6.2
- SUSE Linux Enterprise Server 11 SP2
- Novel Open Enterprise Server 11
- OpenSUSE Linux 12.1
- OpenSUSE Linux 12.2
- Mandriva Enterprise Server 5.2

- Ubuntu Server 10.04.2 LTS
- Ubuntu Server 12.04 LTS
- Debian GNU/Linux 6.0.5
- FreeBSD 8.3
- FreeBSD 9.0

64-битные платформы:

- Red Hat Enterprise Linux 6.2 Server
- Red Hat Enterprise Linux 5.8 Server
- Fedora 16
- CentOS-6.2
- SUSE Linux Enterprise Server 11 SP2
- Novel Open Enterprise Server 11
- OpenSUSE Linux 12.1
- OpenSUSE Linux 12.2
- Ubuntu Server 10.04.2 LTS
- Ubuntu Server 12.04 LTS
- Debian GNU/Linux 6.0.5
- FreeBSD 8.3
- FreeBSD 9.0

Программные средства антивирусной защиты для файловых серверов Linux обеспечивают реализацию следующих функциональных возможностей:

- Резидентный антивирусный мониторинг.
- Антивирусное сканирование по команде пользователя или администратора и по расписанию.
- Антивирусная проверка и лечение файлов в архивах.
- Запуск задач по расписанию и/или сразу после загрузки операционной системы.
- Помещение подозрительных и поврежденных объектов на карантин.
- Формирование отчетов в форматах HTML, CSV, PDF и XLS.
- Возможность перехвата и проверки файловых операций на уровне SAMBA.

• Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность.

• Удаленно через веб-браузер управлять антивирусом и настраивать его.

• Централизованно управляться с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Novell Netware

Программные средства антивирусной защиты для файловых серверов Novell Netware функционируютна компьютерах, работающих под управлением операционных систем следующих версий:

- Novell Netware 5.x SP6 или выше,
- 6.0 SP3 или выше,
- 6.5 SP3 или выше.

Программные средства антивирусной защиты для файловых серверов Novell Netware обеспечивают реализацию следующих функциональных возможностей:

• Проверка на присутствие вирусов всех запускаемых и изменяемых файлов, лечение, а при его невозможности – удаление зараженных объектов.

• Последовательную проверку файлов сервера по запросу администратора или по расписанию с заданной частотой, при этом может производиться лечение и/или удаление зараженных объектов.

• Обновление антивирусных баз и распространение обновлений на другие серверы сети Novell NetWare. Обновление может происходить по расписанию, рассылкой на предопределённые серверы. Предусмотрена возможность создания резервных копий обновляемых файлов для обеспечения возможности отката антивирусных баз до предыдущей версии.

• Размещение зараженных или подозрительных файлов в специальном хранилище – карантине. Помещенные на карантин файлы могут быть проанализированы администратором и/или отправлены на исследование в компанию – разработчик антивирусных решений.

• Создание подробных отчетов по результатам проверок ресурсов сервера по требованию, его постоянной защиты и обновления антивирусных баз. Возможность просмотра журналов и вывода их на печать.

• Сохранение резервной копии всех подозрительных или зараженных объектов перед лечением или удалением, что позволяет восстановить данные в случае возникновения сбоев или ошибок при лечении или удалении.

• Информирование администраторов и пользователей о законченных проверках, а также предупреждение о найденных вредоносных объектах средствами сети Novell NetWare и по электронной почте.

Требования к программным средствам антивирусной защиты для серверов

масштаба предприятия и терминальных серверов Windows

Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows функционируют на компьютерах, работающих под управлением операционных систем следующих версий:

32-битные платформы:

- Microsoft Windows Server 2003 Standard Edition с пакетом обновлений 1 или выше.
- Microsoft Windows Server 2003 Enterprise Edition с пакетом обновлений 1 или выше.
- Microsoft Windows Server 2003 R2 Standard Edition и выше.
- Microsoft Windows Server 2003 R2 Enterprise Edition и выше.
- Microsoft Windows Server 2008 Standard Edition.
- Microsoft Windows Server 2008 Enterprise Edition.
- Microsoft Windows Server 2008 Data Center Edition.
- Microsoft Windows Server 2008 Core Standard Edition.
- Microsoft Windows Server 2008 Core Enterprise Edition.
- Microsoft Windows Server 2008 Core Data Center Edition.

64-битные платформы:

- Microsoft Windows Server 2003 x64 Standard Edition.
- Microsoft Windows Server 2003 x64 Enterprise Edition.
- Microsoft Windows Server 2003 R2 Standard x64 Edition.
- Microsoft Windows Server 2003 R2 Enterprise x64 Edition.
- Microsoft Windows Server 2008 x64 Standard Edition.
- Microsoft Windows Server 2008 x64 Enterprise Edition.
- Microsoft Windows Server 2008 x64 Data Center Edition.
- Microsoft Windows Server 2008 Core x64 Standard Edition.
- Microsoft Windows Server 2008 Core x64 Enterprise Edition.
- Microsoft Windows Server 2008 Core x64 Data Center Edition.
- Microsoft Windows Server 2008 R2 Standard Edition Release с пакетом обновлений SP1.
- Microsoft Windows Server 2008 R2 Enterprise Edition Release с пакетом обновлений SP1.

- Microsoft Windows Server 2008 R2 Datacenter Edition Release с пакетом обновлений SP1.

- Microsoft Windows Server 2008 R2 Core Standard Edition Release с пакетом обновлений SP1.

- Microsoft Windows Server 2008 R2 Core Enterprise Edition Release с пакетом обновлений SP1.

- Microsoft Windows Server 2008 R2 Core Datacenter Edition Release с пакетом обновлений SP1.

- Microsoft Windows Hyper-V Server 2008 R2 Release с пакетом обновлений SP1.

Терминальные серверы:

- Microsoft Terminal на базе Windows 2003 Server.

- Microsoft Terminal на базе Windows Server 2008.

- Microsoft Terminal на базе Windows Server 2008 R2.

- Citrix Presentation Server 4.0.

- Citrix Presentation Server 4.5.

- Citrix XenApp 4.5.

- Citrix XenApp 5.0.

- Citrix XenApp 6.0.

Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

• Осуществление антивирусной проверки на серверах, выполняющих разные функции: Серверов терминалов и принт-серверов; Серверов приложений и контроллеров доменов; Файловых серверов.

- Возможность использования для защиты кластера серверов.

• Проверка следующих объектов защищаемого сервера при доступе к ним: Файлов при их записи и считывании; Альтернативных потоков файловых систем (NTFS-streams); Главной загрузочной записи и загрузочных секторов локальных жестких дисков и съемных носителей.

• Предотвращение вирусных эпидемий за счет фиксации возникновения вирусных атак.

• Восстановление после заражения путем удаления всех связанных с ликвидированным вредоносным объектом записей в системных файлах и реестре ОС, что предотвращает возможные сбои в работе операционной системы.

• Непрерывное отслеживание попыток выполнения на защищаемом сервере

скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или ActiveScripting). Проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.

• Проверка по требованию, заключающаяся в однократной полной или выборочной проверке на наличие угроз объектов на сервере.

• Помещение подозрительных и поврежденных объектов на карантин.

• При защите терминальных серверов поддержка режимов публикации рабочего стола и публикации приложений.

• Масштабируемость за счет задания количества рабочих процессов антивируса для ускорения обработки запросов к серверу при использовании многопроцессорных серверов.

• Балансировка загрузки путем регулирования распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: антивирусная проверка может продолжаться в фоновом режиме.

• Выбор доверенных процессов путем исключения из проверки безопасных процессов, работа которых может замедляться при антивирусной проверке (процесс резервного копирования данных, программы дефрагментации жесткого диска и другие).

• Разделение прав администраторов, основанное на стандартных механизмах ОС Microsoft Windows.

• Уведомления различными методами администраторов и пользователей о событиях в антивирусной защите. Поддержка Simple Network Management Protocol (SNMP).

• Совместимость с системами управления дисковым пространством (Hierarchical Storage Management), позволяющая настраивать способы проверки для Offline Files.

• Оптимизация для использования на многопроцессорных серверах на базе технологии IntelXeon™, позволяющая использовать приложение в условиях высоких нагрузок.

• Возможность управления с помощью MMC консоли.

• Централизованно управляться с помощью единой системы управления.

Требования к программным средствам антивирусной защиты смартфонов

Программные средства для антивирусной защиты смартфонов функционируют под управлением следующих мобильных ОС:

• Android 1.5, 1.6, 2.0, 2.1, 2.2, 2.3, 4.0, 4.1, 4.2

• Apple iOS 4.0, 4.1, 4.2, 4.3, 5.0, 5.1, 6.0, 6.1

• BlackBerry 4.5, 4.6, 4.7, 5.0, 6.0, 7.0, 7.1

- Windows Mobile 5.0, 6.0, 6.1, 6.5
- Symbian 9.1, 9.2, 9.3, 9.4 Series UI 60 и Symbian3, Symbian Anna, Symbian Belle

Программные средства для антивирусной защиты смартфонов должны обеспечивать следующую функциональность:

- Постоянная защита файловой системы смартфона, включающая перехват и проверку:
- • Всех входящих объектов, передающихся с помощью беспроводных соединений (инфракрасный порт, Bluetooth), сообщений EMS и MMS, при синхронизации с персональным компьютером и загрузке файлов через браузер.
- • Файлов, открываемых на смартфоне.
- • Программ, устанавливаемых из интерфейса смартфона.
- Проверка объектов файловой системы, находящихся на смартфоне или на подключенных картах расширения памяти, по требованию пользователя и по расписанию.
- Надежное изолирование зараженных объектов в карантинном хранилище.
- Обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов.
- Блокирование нежелательных SMS и MMS сообщений.
- Шифрование наиболее важных файлов, папок и карты памяти.
- Возможность скрывать важные контакты и историю общения с ними.
- Осуществление функции «антивор», т.е. возможность блокировки мобильного устройства, удаление данных, сообщений и книги контактов, получение координат местоположения, а также определение, у кого находится пропавшее устройство.

Требования к программным средствам централизованного управления, мониторинга и обновления

Программные средства централизованного управления, мониторинга и обновления функционируют на компьютерах, работающих под управлением операционных систем следующих версий:

Сервер администрирования:

- Microsoft Windows XP Professional SP2 и выше
- Microsoft Windows XP Professional x64 и выше
- Microsoft Windows Server 2003 и выше
- Microsoft Windows Server 2003 x64 и выше
- Microsoft Windows Vista SP1 и выше

- Microsoft Windows Vista x64 SP1 и всеми текущими обновлениями
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008, развернутая в режиме Server Core
- Microsoft Windows Server 2008 x64 SP1 и всеми текущими обновлениями
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Small Business Server 2003
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2011
- Microsoft Windows 7 Professional/Enterprise/Ultimate
- Microsoft Windows 7 Professional/Enterprise/Ultimate x64
- Microsoft Windows 8
- Microsoft Windows 8 x64

Консоль администрирования:

- Microsoft Windows XP Professional SP2 и выше
- Microsoft Windows XP Professional x64 и выше
- Microsoft Windows Server 2003 и выше
- Microsoft Windows Server 2003 x64 и выше
- Windows Small Business Server 2003
- Microsoft Windows Vista SP1 и выше
- Microsoft Windows Vista x64 SP1 и всеми текущими обновлениями
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 x64 SP1 и всеми текущими обновлениями
- Windows Small Business Server 2008 x64
- Microsoft Windows Server 2008 x64 R2
- Microsoft Windows Server 2008 x64 R2 SP1
- Windows Small Business Server 2011 x64
- Microsoft Windows 8

- Microsoft Windows 8 x64
- Microsoft Windows 7 Professional/Enterprise/Ultimate SP1
- Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1

Агент администрирования:

• Программные требования для агента администрирования, устанавливаемого на защищаемый компьютер, должны соответствовать требованиям к соответствующим программным средствам антивирусной защиты.

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

- Microsoft SQL Express 2005
- Microsoft SQL Express 2008
- Microsoft SQL Express 2008 R2
- Microsoft SQL Express 2012
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- MySQL 5.0.67, 5.0.77, 5.0.85, 5.0.87(SP1), 5.0.91
- MySQL Enterprise 5.0.60(SP1), 5.0.70, 5.0.82(SP1), 5.0.90

Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий:

- VMware (Workstation 6.0 и Esxi 4.0)
- Microsoft Hyper-V
- KVM интегрированный с Ubuntu 10.10
- Microsoft Virtual PC 6.0.156.0
- Parallels 4.0.6630
- Oracle Virtual Box 4.0.4-70112 (поддерживается только гостевой вход для Windows)
- Citrix Xen Server 5.6.1 FP1

Программные средства управления для всех защищаемых ресурсов должны

обеспечивать реализацию следующих функциональных возможностей:

- Установка системы антивирусной защиты из единого дистрибутива.

- Выбор установки в зависимости от количества защищаемых узлов.

- Создание групп логической сети на основе структуры Active Directory.

- Автоматическое распределение компьютеров по группам управления, в случае появления новых компьютеров в сети.

- Централизованные установка, обновление и удаление программных средств антивирусной защиты, настройка, администрирование, просмотр отчетов и статистической информации по их работе.

- Централизованное удаление несовместимых приложений.

- Централизованное управление установкой и запуском программ на компьютерах пользователей с возможностью контроля программ по пути нахождения программы, метаданным, MD5 контрольной сумме и возможностью присвоения привилегий определенным пользователям.

- Централизованное управление доступом к веб-ресурсам с компьютеров пользователей, с возможностью фильтрации по категориям и типу данных загружаемого контента, гибко задавать параметры времени действия правил и возможностью присвоения привилегий определенным пользователям.

- Наличие различных методов установки антивирусных приложений: для удаленной установки - RPC, GPO, агент администрирования, для локальной установки - автономный пакет установки.

- Удаленная установка программных средств антивирусной защиты с последней версией баз приложения.

- Автоматизированное обновление программных средств антивирусной защиты и антивирусных баз.

- Автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей.

- Тестирование загруженных обновлений средствами сервера администрирования перед распространением на клиентские машины; доставку обновлений на рабочие места пользователей сразу после их получения.

- Распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере.

- Централизованный контроль работы пользователя с внешними устройствами ввода/вывода, с возможностью ограничения доступа к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных, с возможностью создавать доверенные устройства по их идентификатору и возможностью предоставлять привилегии, для запуска внешних устройств, определенным пользователям.

• Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне.

- Создание виртуальных серверов управления антивирусным приложением.

- Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации.

- Доступ к облачным серверам производителя антивирусного ПО через сервер управления.

- Автоматическое распространение лицензии на клиентские компьютеры.

• Централизованный сбор информации и создание отчетов о состоянии антивирусной защиты.

- Инвентаризация установленного ПО и оборудования на компьютерах пользователей.

• Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройку рассылки почтовых уведомлений о них.

- Функция для управления мобильными устройствами через сервер Exchange ActiveSync.

- Функция для управления мобильными устройствами через сервер iOS MDM.

- Возможность отправки SMS-сообщений мобильным пользователям.

- Централизованная установка приложений на управляемые мобильные устройства.

- Централизованная установка сертификатов на управляемые мобильные устройства.

- Централизованный сбор информации о всех установленных на клиентских компьютерах приложениях.

- Интеграция с CISCO NAC и MS NAP.

- Экспорт отчетов в файлы форматов PDF и XML.

• Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение.

- Создание внутренних учетных записей для аутентификации на сервере управления.

- Создание резервной копии системы управления.

- Поддержка Windows Failover Clustering.

- Наличие веб-консоли управления приложением.

- Наличие системы контроля возникновения вирусных эпидемий.

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных обеспечивают реализацию следующих функциональных возможностей:

- Регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток, а баз антиспама не реже одного раза в 5 минут.

- Множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации.

- Проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

- Руководство пользователя (администратора).

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты

Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

- Предоставляться 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 АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов.

В соответствии с пунктом 2 части 1 статьи 64 Закона о контрактной системе документация об электронном аукционе наряду с информацией, указанной в извещении о проведении такого аукциона, должна содержать, в том числе требования к содержанию, составу заявки на участие в таком аукционе в соответствии с частями 3 - 6 статьи 66 настоящего Федерального закона и инструкцию по ее заполнению. При этом не допускается установление требований, влекущих за собой ограничение количества участников такого аукциона или ограничение доступа к участию в таком аукционе.

Частью 2 статьи 66 Закона о контрактной системе установлено, что заявка на участие в электронном аукционе состоит из двух частей.

Согласно подпункту б) пункта 1 части 3 статьи 66 Закона о контрактной системе первая часть заявки на участие в электронном аукционе при заключении контракта на поставку товара должна содержать конкретные показатели, соответствующие значениям, установленным документацией о таком аукционе, и указание на товарный знак (его словесное обозначение) (при наличии), знак обслуживания (при наличии), фирменное наименование (при наличии), патенты (при наличии), полезные модели (при наличии), промышленные образцы (при наличии), наименование страны происхождения товара.

Аналогичное подпункту б) пункта 1 части 3 статьи 66 Закона о контрактной системе требование к содержанию первой части заявки на участие в электронном аукционе при заключении контракта на поставку товара определено подпунктом 1б части 3 пункта 12 раздела I документации об электронном аукционе.

Пунктом 27 «Требования к содержанию, составу первой части заявки на участие в электронном аукционе» раздела II «Информационная карта» документации об электронном аукционе (далее - Информационная карта), техническим заданием определено: «Первая часть заявки на участие в электронном аукционе в соответствии с требованиями документации об электронном аукционе и Федерального закона от 05.04.2013 г. № 44-ФЗ должна содержать:

- информацию, предусмотренную п/п б) п.1) ч. 3 п. 12 раздела I документации об аукционе, а именно: *конкретные показатели* (наименование, характеристики товара, в том числе требования к программному обеспечению, количество), соответствующие значениям, установленным в Описании объекта закупки, а также указание на товарный знак (его словесное обозначение) (при его наличии), знак обслуживания (при наличии), фирменное наименование (при наличии), патенты (при наличии), полезные модели (при наличии), промышленные образцы (при наличии), наименование страны происхождения товара.

В силу частей 1, 3-6 статьи 67 Закона о контрактной системе аукционная комиссия проверяет первые части заявок на участие в электронном аукционе, содержащие информацию, предусмотренную частью 3 статьи 66 настоящего Федерального закона, на соответствие требованиям, установленным документацией о таком аукционе в отношении закупаемых товаров, работ, услуг.

По результатам рассмотрения первых частей заявок на участие в электронном аукционе, содержащих информацию, предусмотренную частью 3 статьи 66 настоящего Федерального закона, аукционная комиссия принимает решение о допуске участника закупки, подавшего заявку на участие в таком аукционе, к участию в нем и признании этого участника закупки участником такого аукциона или об отказе в допуске к участию в таком аукционе в порядке и по основаниям, которые предусмотрены частью 4 настоящей статьи.

Участник электронного аукциона не допускается к участию в нем в случае:

1) непредоставления информации, предусмотренной частью 3 статьи 66 настоящего Федерального закона, или предоставления недостоверной информации;

2) несоответствия информации, предусмотренной частью 3 статьи 66 настоящего

Федерального закона, требованиям документации о таком аукционе.

Отказ в допуске к участию в электронном аукционе по основаниям, не предусмотренным частью 4 настоящей статьи, не допускается.

В соответствии с ч.3 ст. 65 Закона о контрактной системе любой участник электронного аукциона, получивший аккредитацию на электронной площадке, вправе направить на адрес электронной площадки, на которой планируется проведение такого аукциона, запрос о даче разъяснений положений документации о таком аукционе. При этом участник такого аукциона вправе направить не более чем три запроса о даче разъяснений положений данной документации в отношении одного такого аукциона. В течение одного часа с момента поступления указанного запроса он направляется оператором электронной площадки заказчику.

Как следует из пояснений представителя заказчика, заявка ООО «СИСТЕМЫ ПЛЮС» не соответствовала требованиям документации об электронном аукционе.

Согласно устным доводам представителя заказчика, заявитель в данном случае ООО «СИСТЕМЫ ПЛЮС» правом на дачу разъяснений положений документации не воспользовался.

По результатам рассмотрения первых частей заявок на участие в электронном аукционе аукционная комиссия оформляет протокол рассмотрения заявок на участие в таком аукционе, подписываемый всеми присутствующими на заседании аукционной комиссии ее членами не позднее даты окончания срока рассмотрения данных заявок.

Указанный протокол должен содержать информацию:

1) о порядковых номерах заявок на участие в таком аукционе;

2) о допуске участника закупки, подавшего заявку на участие в таком аукционе, которой присвоен соответствующий порядковый номер <...> к участию в таком аукционе и признании этого участника закупки участником такого аукциона или об отказе в допуске к участию в таком аукционе с обоснованием этого решения, в том числе с указанием положений документации о таком аукционе, которым не соответствует заявка на участие в нем, положений заявки на участие в таком аукционе, которые не соответствуют требованиям, установленным документацией о нем;

3) о решении каждого члена аукционной комиссии в отношении каждого участника такого аукциона о допуске к участию в нем и о признании его участником или об отказе в допуске к участию в таком аукционе.

На участие в электронном аукционе, предметом которого являлась «Поставка антивирусного программного обеспечения» было подано три заявки.

Заявке ООО «СИСТЕМЫ ПЛЮС» на участие в электронном аукционе оператором электронной площадки присвоен порядковый номер <...> .

Комиссией Коми УФАС России на заседании установлено, что в соответствии с протоколом рассмотрения первых частей заявок на участие в электронном

аукционе от 29.07.2016, заявка участника с порядковым номером два не соответствует предъявляемым требованиям заказчика.

Таким образом, сведения, содержащиеся в первой части заявки с порядковым номером 2 на участие в электронном аукционе, не соответствуют требованиям, установленным документацией об электронном аукционе, а именно: требованиям, установленным пунктом 27 Информационной карты, Техническим заданием документации об электронном аукционе.

Аукционной комиссией по результатам рассмотрения первой части заявки с порядковым номером 2 на участие в электронном аукционе принято решение об отказе в допуске к участию в электронном аукционе участника закупки, подавшего указанную заявку, на основании пункта 1 части 4 статьи 67 Закона о контрактной системе с обоснованием принятого решения: «Сведения, содержащиеся в первой части заявки на участие в электронном аукционе, не соответствуют требованиям, установленным п/п 1б) ч. 3 п. 12 и п/п 1 ч.3 п.14 раздела I; пункта 27 раздела II; раздела III (Техническое задание) документации об электронном аукционе, а именно не представлены конкретные показатели предлагаемого для поставки товара, установленные документацией об аукционе.

Данное решение отражено в протоколе от 29.07.2016 № 0307200008716000200-1 рассмотрения первых заявок на участие в электронном аукционе.

Действия аукционной комиссии в виде принятия решения об отказе в допуске к участию в электронном аукционе участника закупки, подавшего заявку с порядковым номером 2 на участие в электронном аукционе правомерны и соответствуют пункту 1 части 4 статьи 67 Закона о контрактной системе.

С учетом всех вышеизложенных обстоятельств, руководствуясь частью 8 статьи 106 Закона о контрактной системе, Комиссия Коми УФАС России

РЕШИЛА:

1. Признать жалобу ООО «СИСТЕМЫ ПЛЮС» необоснованной.

Решение может быть обжаловано в судебном порядке в течение трех месяцев со дня его принятия.

Председатель Комиссии <……..>

Члены комиссии <……..>