УТВЕРЖДАЮ
Директор ГИН РАН

_____ К.Е.Дегтярев

# Техническое задание

**Наименование объекта закупки:** Поставка лицензий на антивирусное программное обеспечение.

| Наименование программного обеспечения |
|---|
| Лицензия (простая неисключительная лицензия) на антивирусный программный продукт Dr.Web Desktop Security Suite (Комплексная защита) + Центр управления на 201 рабочую станцию с поддержкой в течение 12 месяцев. Продление.<br>Код продукта: LBW-BC-12M-201-B3-FST |
| Расширение лицензии для Dr.Web Enterprise Security Suite сертифицированный ФСТЭК России (электронный сертификат ФСТЭК № 3509) с поддержкой в течение 12 месяцев.<br>Код продукта: CERT-FST |

Примечание: В соответствии с п. 1 ч. 1 ст. 33 Федерального закона от 05 апреля 2013 года №44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в связи с необходимостью обеспечения взаимодействия поставляемого программного обеспечения с программным обеспечением, используемым Заказчиком, эквивалент на указанное программное обеспечение отсутствует (не предусмотрен).

## 1 Общие требования

**1.1** Участники конкурса на использование антивирусного программного продукта должны иметь статус официального партнера компании производителя, что является подтверждением их квалификации и прав на поставку антивирусных продуктов и/или лицензий. При заключении контракта необходимо предоставить копии документов, подтверждающих статус официального партнера компании производителя.

**1.2** Участник должен принять во внимание, что ссылка на наименование продукции носит описательный, а не обязательный характер. В случае если Участником предлагаются эквивалент требуемого Заказчиком ПО, то в составе своей конкурсной заявки он должен в обязательном порядке предоставить следующую информацию:

**1.2.1** в Техническом предложении – подробное техническое описание предлагаемого к поставке эквивалента, с указанием полного соответствия (или превосходящего) всем техническим характеристикам, указанным в данной спецификации, заверенное у производителя предлагаемого программного продукта

Отсутствие в составе конкурсной заявки подробного технического описания аналогов продукции и/или письма о согласовании может являться причиной отклонения конкурсной заявки Участника.

**1.3** Все компоненты Системы должны принадлежать одной торговой марке с единой службой технической поддержки на русском языке. Техническая поддержка должна предоставляться непосредственно производителем поставляемых программных продуктов.

**1.4** В рамках всей организации должны использоваться единые антивирусные средства независимо от степени конфиденциальности обрабатываемой информации. Отдельно стоящие ПК, не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от проникновения и активации всех типов вредоносных программ (антивирус), спама (персональный антиспам) и обеспечивать возможность их включения в единую систему антивирусной защиты.

**1.5** Поставляемые средства защиты должны представлять масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети заказчика.

**1.6** Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке.

**1.7** Все антивирусные средства, функционирующие под операционной системой типа Windows, включая средства управления, должны обладать контекстной справочной системой на русском языке.

**1.8** Участник конкурса должен предоставить единый серийный номер для всех поставляемых по условиям конкурса продуктов.

**1.9** Поставляемый серийный номер должен иметь возможность отложенной активации. Срок действия лицензионных ключевых файлов на все поставляемые по условиям конкурса программные продукты должен начинаться с момента активации серийного номера.

**1.10** Система лицензирования не должна иметь привязку к используемому на защищаемых объектах аппаратному обеспечению. Система должна позволять перенос лицензий с одних защищаемых объектов (в том числе рабочих станций и серверов) на иные без необходимости перепривязки или получения дополнительных лицензий

**1.11** Антивирусные средства должны включать:

- программные средства защиты рабочих станций и файловых серверов;
- программные средства централизованного управления, мониторинга и обновления;
- обновляемые базы данных сигнатур вредоносных программ всех типов и атак;
- эксплуатационную документацию на русском языке.

## 2 Требования к программным средствам

### 2.1 Общие требования к системе антивирусной защиты

**2.1.1** Программные средства Системы должны обеспечивать определение угроз следующих типов:

**2.1.2** классических вирусов;

**2.1.3** троянских программ;

**2.1.4** руткитов;

**2.1.5** сетевых червей;

**2.1.6** рекламных программ;

**2.1.7** программ автодозвона на платные сайты;

**2.1.8** потенциально опасных приложений;

**2.1.9** прочих вредоносных программ.

**2.1.10** Антивирусная защита должна обеспечивать:

**2.1.11** обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п.;

**2.1.12** обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками;

**2.1.13** 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;

**2.1.14** обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME);

**2.1.15** обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т.д.);

**2.1.16** 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);

**2.1.17** 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;

**2.1.18** проверку упакованных файлов следующих форматов: PELOCK, ENIGMA, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, а также почтовых файлов Mozilla Thunderbird большого размера;

**2.1.19** разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF;

**2.1.20** защиту от еще неизвестных вредоносных программ, принадлежащих зарегистрированным семействам, как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;

**2.1.21** 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;

**2.1.22** обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA);

**2.1.23** обнаружение угроз, направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля

**2.1.24** обнаружение вредоносных объектов в DEX-файлах (Android).

**2.1.25** Используемое антивирусное ядро:

**2.1.26** не должно допускать снижение скорости проверки при увеличении размера антивирусных баз;

**2.1.27** в целях оптимального расхода ресурсов должно, в зависимости от загрузки системы, выбирать уровень анализа упакованных объектов;

**2.1.28** в целях оптимального расхода ресурсов должно использовать механизм уменьшения размера промежуточных файлов;

**2.1.29** в целях ускорения проверки архивов и упакованных файлов должно обеспечивать опознание вредоносных программ без запуска распаковщика;

**2.1.29.1** должно обеспечивать защиту от так называемых «почтовых бомб»;

**2.1.29.2** должно обеспечивать работу с файлами больше 2 ГБ;

**2.1.29.3** должно поддерживать работу с дисками с LBA-адресацией;

**2.1.29.4** в целях исключения «утечки» оперативной памяти должно использовать механизм распределения динамической памяти уровня ядра.

## 2.2 Требования к системе управления антивирусной защитой (далее - Сервер управления)

**2.2.1** Система управления должна быть построена по клиент-серверной архитектуре с возможностью построения иерархической системы серверов – с возможностью использования в системе антивирусного управления как главных, так подчиненных серверов. Система управления должна иметь возможность установки на ОС Microsoft Windows, FreeBSD, Solaris, а также на ОС типа Linux.

**2.2.2** Система управления должна быть реализована на основе Web-интерфейса, поддерживающего стандартно используемые Web-браузеры, в том числе Mozilla Firefox или Internet Explorer.

**2.2.3** Система должна включать поддержку кластерного протокола, с помощью которого координируются действия над агентами защиты с разных антивирусных серверов

**2.2.4** Система управления должна быть доступной с любой операционной системы, поддерживающей браузеры Mozilla Firefox или Internet Explorer (в том числе с ОС Microsoft Windows и ОС типа UNIX (Linux, FreeBSD, Solaris)), без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения как на стороне сервера управления, так и на стороне администратора Системы. Контроль работы Системы должен быть также возможен консоли управлеия, функционирующей на мобильных устройствах iPhone

**2.2.5** В целях безопасности все ПО, входящее в состав антивирусного сервера (в том числе необходимое для доступа с помощью браузера) должно поставляться в виде единого дистрибутива и принадлежать одной торговой марке.

**2.2.6** Система управления должна включать систему управления лицензиями, позволяющую распределять между серверами в рамках иерархической сети необходимое количество лицензий

**2.2.7** Установка антивирусного сервера Системы должна быть возможна на:

**2.2.8** Microsoft Windows 2000 Professional и Server;

**2.2.9** Microsoft Windows XP Professional и Home Edition;

**2.2.10** Microsoft Windows Server 2003;

**2.2.11** Microsoft Windows 10

**2.2.12** Microsoft Windows 11

**2.2.13** Microsoft Windows Vista;

**2.2.14** Microsoft Windows Server 2008;

**2.2.15** Microsoft Windows 7;

**2.2.16** Microsoft Windows Server 2012;

**2.2.17** Microsoft Windows 8.

**2.2.18** Linux glibc2.7 и выше, в том числе Astra Linux 1.7, Astra Linux 1.8

**2.2.19** FreeBSD 7.3 и выше

**2.2.20** Sun Solaris 10 x86 и Sparc

**2.2.21** Установка агента управления антивирусной защиты должна быть возможна на:

**2.2.22** Linux glibc 2.7 и выше, в том числе Astra Linux 1.7, Astra Linux 1.8

**2.2.23** FreeBSD 7.3 и выше

**2.2.24** Sun Solaris 10 (только для платформы Intel)

**2.2.25** Microsoft Windows 98/Millennium Edition

**2.2.26** Microsoft Windows NT4 (SP6a)

**2.2.27** Microsoft Windows 2000 Professional (SP4 также с Update Rollup 1)

**2.2.28** Microsoft Windows 2000 Server (SP4 также с Update Rollup 1)

**2.2.29** Microsoft Windows XP Professional (также с SP1 и выше)

**2.2.30** Microsoft Windows XP Home (также с SP1 и выше)

**2.2.31** Microsoft Windows Server 2003 (также с SP1 и выше)

**2.2.32** Microsoft Windows Vista (также с SP1 и выше)

**2.2.33** Microsoft Windows Server 2008 (также с SP1 и выше)

**2.2.34** Microsoft Windows 7

**2.2.35** Microsoft Windows Server 2012

**2.2.36** Microsoft Windows 8

**2.2.37** Microsoft Windows Mobile 2003/2003 Second Edition/5.0/6.0/6.1/6.5

**2.2.38** ОС Android 1.6/2.0/2.1/2.2/2.3/3.0/3.1/3.2/4.0;

**2.2.39** Mac OS X 10.6 и выше.

**2.2.40** Система управления должна иметь возможность:

**2.2.41** просмотра и сравнения состава аппаратно-программного обеспечения на станциях антивирусной сети

**2.2.42** контроля неактивных станций антивирусной сети

**2.2.43** просмотра сессий пользователей антивирусной сети

**2.2.44** замены системного DNS

**2.2.45** использования как внутренней СУБД (поставляемой в составе дистрибутива антивирусного сервера), так и внешней (устанавливаемой отдельно до или после развертывания антивирусного сервера). При использовании внешней СУБД Система должна иметь возможность работы с ней как без установки дополнительное ПО (с СУБД MS SQL CE, Oracle), так и с помощью драйверов ODBC для операционных систем Windows и Linux (в том числе с СУБД PostgreSQL). Система должна иметь возможность замены типа используемой СУБД после установки серверной части – без необходимости переустановки серверной части Системы

**2.2.46** управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов

**2.2.47** экспорта и импорта базы данных антивирусного сервера в XML-файл.

**2.2.48** создания иерархической сети антивирусных серверов. В случае реализации иерархической сети Система должна иметь возможность:

**2.2.49** объединения информации от нескольких серверов на одном.

**2.2.50** распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть.

**2.2.51** обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий

**2.2.52** контроля отсутствия связанных серверов в расписании антивирусного сервера.

**2.2.53** построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне;

**2.2.54** установки антивирусных агентов в сети, не использующей единого пароля доступа к рабочим станциям;

**2.2.55** централизованной настройки параметров защиты, уникальных для различных групп, в том числе для рабочих станций, находящихся в режиме off-line.

**2.2.56** централизованного сбора и просмотра статистической информации и создания отчетов о состоянии антивирусной защиты и их консолидации;

**2.2.57** наличия множественных путей уведомления пользователей и администраторов путем посылки почтового сообщения, звукового оповещения, всплывающего окна, записи в журнал событий, SNMP-trap;

**2.2.58** оповещения о возникновении эпидемий (множественных инфекций)

**2.2.59** оповещения о наличии обновлений сервера

**2.2.60** отправки информационных сообщений пользователям по сети в режиме реального времени через Web-интерфейс Системы;

**2.2.61** обеспечения связи антивирусного сервера и клиентских частей через встроенный модуль в случае, когда они расположены в различных сетях, работающих по протоколам TCP/IP (в т.ч. IPv6), IPX/SPX, NetBIOS, между которыми отсутствует маршрутизация пакетов

**2.2.62** самостоятельного написания обработчиков событий на языке Lua, а также выполнения произвольных Lua-скриптов с помощью средств системы управления.

**2.2.63** В случае интеграции с внешними подсистемами с помощью встроенного Web API, должна иметься возможность аудита действий, произведенных с помощью функций данного Web API

**2.2.64** Вне зависимости от типа антивирусного агента и защищаемой системы, Система должна обеспечивать реализацию следующих функциональных возможностей

**2.2.65** экспорта, импорта и распространения конфигураций групп, станций антивирусной сети или компонентов антивирусной защиты на другие группы, станции и компоненты, в том числе в целях изменения политик, применения их к определенным группам

**2.2.66** скачивания конфигурационных файлов с настройками подключения антивирусных агентов для ОС Android, Mac OS X и ОС семейства UNIX

**2.2.67** восстановления рабочих станций, случайно удаленных из системы защиты;

**2.2.68** централизованного обновления антивирусных баз на всех защищенных рабочих станциях, в том числе мобильных и находящихся в режиме off-line. Доставки обновлений на рабочие места пользователей как по расписанию, так сразу после их получения;

**2.2.69** обновления программных средств и антивирусных баз из разных источников, доставляемые как автоматически по каналам связи в пределах антивирусной сети, так и на отчуждаемых машинных носителях информации – путем ручной синхронизации информации между серверами и рабочими станциями

**2.2.70** обновления программных средств и антивирусных баз с помощью мобильного сервера обновлений, представляющего собой Сервер управления, развернутый на flash-диске;

**2.2.71** управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений

**2.2.72** контроля результатов обновления антивирусного ПО на станциях антивирусной сети.

**2.2.73** организации межсерверного обмена согласно расписанию

**2.2.74** ограничения канала связи по группам

**2.2.75** наличия возможности групповых обновлений

**2.2.76** обновлений по защищенному каналу с использованием SSL-сертификатов

**2.2.77** организации отложенного обновления

**2.2.78** проверки обновлений на выбранных администратором компьютерах/группах перед распространением их на все клиентские компьютеры

**2.2.79** автоматического перехода установленного ПО на более новые версии, в том числе с возможностью выбора обновляемых компонентов;

**2.2.80** Программные средства управления для всех защищаемых ресурсов, реализованных на платформах ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:

**2.2.81** централизованной удаленной установки и деинсталляции программных средств, антивирусных баз и антивирусного ядра на защищаемые узлы сети – в том числе на станции, находящиеся в разных доменах.

**2.2.82** создания инсталляционных пакетов для конкретных защищаемых рабочих станций;

**2.2.83** выбора и настройки устанавливаемых компонентов до начала установки антивирусного пакета на клиентские части;

**2.2.84** Система должна обладать 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 через Web-интерфейс, без необходимости использования файлов конфигурации типа *.xml.

**2.2.85** Система управления должна поддерживать возможность:

**2.2.86** создания точки восстановления перед установкой антивирусного пакета на защищаемые рабочие станции и сервера;

**2.2.87** восстановления удаленных станций.

**2.2.88** Система должна поддерживать множественную возможность установки своих компонентов на защищаемые рабочие станции – в том числе с помощью:

**2.2.89** прямого их указания в системе управления в результате сканирования локальной сети, Microsoft Active Directory,

**2.2.90** политик Microsoft Active Directory

**2.2.91** синхронизации станций с Microsoft Active Directory

**2.2.92** установки с помощью дистрибутива, содержащего все компоненты защиты

**2.2.93** рассылки инсталляционных файлов из системы управления по электронной почте

**2.2.94** возможностей службы распределенной файловой системы (DFS).

**2.2.95** Система должна поддерживать возможность настройки правил автоматического распределения станций по пользовательским группам, а также возможность изменения первичной группы при автоматическом подтверждении доступа станций к антивирусному серверу

**2.2.96** Система управления должна обладать 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.

**2.2.97** Система должна иметь возможность минимизации трафика:

**2.2.97.1** за счет применения специальных алгоритмов сжатия;

**2.2.97.2** ограничения трафика по пропускной способности и по времени в определенных IP-подсетях.

**2.2.98** Система должна иметь возможность интеграции с платформой Microsoft® Network Access Protection (NAP), обеспечивающей автоматическую систему реагирования на инциденты безопасности.

**2.2.99** Система должна иметь возможность выбора уровня подробности протоколирования своих компонентов. система управления должна иметь возможность загрузки архивированных файлов журнала работы всех антивирусных серверов иерархической сети

**2.2.100** В целях ограничения использования серверного пространства должна иметься возможность ротации файлов журнала антивирусного сервера по времени (час, день, неделя)

**2.2.101** Система управления должна обеспечивать защиту от несанкционированного доступа. Авторизация должна обеспечиваться парой логин/пароль.

**2.2.102** Администраторы Системы должны иметь возможность авторизации с помощью ActiveDirectory, LDAP, RADIUS, PAM. Система управления должна иметь возможность предварительного тестирования настроек авторизации внешних администраторов Active Directory, LDAP и RADIUS

**2.2.103** Система должна иметь журнал аудита действий администраторов Системы, позволяющий просматривать журнал событий и изменений, осуществленных администраторами при помощи системы управления.

**2.2.104** Система должна обеспечивать:

**2.2.104.1** возможность экспорта выбранных файлов из карантина рабочей станции и/или файлового сервера на антивирусный сервер для дальнейшего анализа;

**2.2.104.2** возможность задания групповых политик в зависимости от группы IP-адресов.

**2.2.104.3** возможность просмотра новостей безопасности, в том числе информирующих об актуальных угрозах

**2.2.105** В случае включения какого-либо компонента Системы в единую систему управления антивирусной защиты локальной сети:

**2.2.106** обновления компонента Системы должны происходить через сервер обновления системы управления антивирусной защиты;

**2.2.107** статистика работы компонентов Системы должна:

**2.2.108** собираться на сервере системы управления антивирусной защиты;

**2.2.109** быть доступной с любой операционной системы, поддерживающей браузеры Mozilla Firefox, Internet Explorer, Safari, Opera без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения за исключением устанавливаемого автоматически с антивирусного сервера модуля, необходимого для отображения статистики.

**2.2.110** Иметь возможность экспорта в формат PDF

**2.2.110.1.1** Иметь возможность отправки по электронной почте согласно расписанию работы антивирусного сервера

**2.2.111** Система должна обеспечивать реализацию следующих функциональных возможностей по обновлению:

**2.2.111.1** получения ежедневных обновлений вирусных баз не менее 10 раз в сутки независимо от того, рабочий, либо выходной день, что должно подтверждаться созданным Системой отчетом (файлом протокола). Система также должна поддерживать возможность получения экстренных обновлений, связанных с выходом новых типов вредоносного ПО, а также возможность мгновенного распространения этих обновлений;

**2.2.111.2** возможность множественности путей обновления, в том числе по каналам связи и на съемных электронных носителях информации;

**2.2.111.3** возможность обновления через прокси-серверы, в том числе прокси-серверы MS ISA/TMG.

**2.2.111.4** проверка целостности и подлинности обновлений средствами электронной цифровой подписи.

**2.2.112** в Системе, не имеющей доступа к сети Интернет, должна быть реализована возможность обновления вирусных баз путём скачивания их с сервера разработчика Системы с возможностью последующего их переноса в Систему с помощью любого носителя информации, в том числе с помощью мобильного сервера обновлений, созданного на основе flash-диска;

**2.2.113** В случае размещения антивирусных серверов во внутренней сети без доступа к сети Интернет получение обновлений должно быть возможно с помощью специальной утилиты автономной загрузки репозитория;

**2.2.114** Система должна иметь возможность перезагрузки защищаемой станции через систему управления

**2.2.115** Система должна иметь возможность шифрования трафика между серверами и защищаемыми рабочими станциями в целях предотвращения утечки конфиденциальной информации.

**2.3 Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows**

**2.3.1** Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:

**2.3.2** осуществление антивирусной (включая постоянную защиту от руткит-технологий) и антиспам защиты на рабочих станциях.

**2.3.3** Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов:

**2.3.4** Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию, должна обеспечивать защиту рабочих станций под управлением операционных систем:

**2.3.4.1** Microsoft Windows 98 / ME;

**2.3.4.2** Microsoft Windows NT Workstation 4.0 (Service Pack 6a);

**2.3.4.3** Microsoft Windows 2000 Professional и Server;

**2.3.4.4** Microsoft Windows XP Professional и Home Edition;

**2.3.4.5** Microsoft Windows Server 2003;

**2.3.4.6** Microsoft Windows Vista;

**2.3.4.7** Microsoft Windows Server 2008;

**2.3.4.8** Microsoft Windows 7;

**2.3.4.9** Microsoft Windows Server 2012;

**2.3.4.10** Microsoft Windows 8.

**2.3.5** Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки без существенного снижения производительности защищаемых рабочих станций. 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.

**2.3.6** 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.

**2.3.7** 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.

**2.3.8** В случае наличия системы централизованного управления права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля.

**2.3.9** 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.

**2.3.10** В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.

**2.3.11** 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.

**2.3.12** Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:

**2.3.12.1** поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;

**2.3.12.2** непрерывное фоновое сканирование в целях нейтрализации активных угроз

**2.3.12.3** проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;

**2.3.12.4** 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;

**2.3.12.5** блокировку опасных макросов VBA в реальном времени;

**2.3.12.6** защиту от вредоносных сценариев, загружаемых с Web-страниц;

**2.3.12.7** защиту от проникновения вредоносных программ и использования уязвимостей за счет использования персонального межсетевого экрана;

**2.3.12.8** проверку трафика как до получения его программными клиентами, так и после, с целью исключения использования уязвимостей прикладного ПО;

**2.3.12.9** 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;

**2.3.12.10** ограничения доступа к сети Интернет или к компьютеру в определенный момент времени по расписанию

**2.3.12.11** помещение найденных зараженных файлов в специальное место на жестком диске - «карантин»;

**2.3.12.12** просмотр местоположения станций и серверов на карте, если заданы географические координаты станции

**2.3.12.13** автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;

**2.3.12.14** запуск задач по расписанию и/или сразу после загрузки операционной системы;

**2.3.12.15** возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке.

**2.3.13** Система защиты рабочих станций должна обеспечивать проверку протоколов:

**2.3.14** HTTP;

**2.3.15** IMAP, SMTP, POP3 независимо от используемого почтового клиента;

**2.3.15.1** NNTP (только проверка на вирусы), независимо от почтового клиента.

**2.3.16** 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:

**2.3.16.1** антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;

**2.3.16.2** проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.

**2.3.17** 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.

**2.3.18** Система должна обеспечивать защиту от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе семейств Trojan.Encoder, Trojan.Inject и Trojan.Winlock) с помощью превентивной защиты, отслеживающей попытки внедрения вредоносных файлов

**2.3.19** В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.

## 2.4 Требования к программным средствам антивирусной защиты рабочих станций Linux

**2.4.1** Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.

**2.4.2** Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.

**2.4.3** Система, используя актуальную на момент проведения тендера версию, должна обеспечивать защиту ресурсов рабочих станций, функционирующих под управлением операционных систем:

**2.4.3.1** Linux, имеющих версию ядра 2.6.x и выше

**2.4.4** Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью универсального пакета для UNIX систем, независимого от типа и версии используемой операционной системы, репозитория или пакета, рассчитанного на работу с используемым в ОС менеджером пакетов

**2.4.5** Установка и обновление Системы должны быть возможны как через средства командной строки, так и с помощью графического инсталлятора.

**2.4.6** Система установки должна включать возможность автоматической установки модулей, необходимых для компонентов Системы.

**2.4.7** Компоненты Системы должны устойчиво функционировать на серверах в условиях их минимальной и максимальной загрузки без существенного снижения производительности.

**2.4.8** Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности работы. При этом, в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках имеющихся у них прав.

**2.4.9** Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением заданных файловых областей.

**2.4.10** Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:

**2.4.10.1** поиск и удаление вирусов всех известных типов в файлах;

**2.4.10.2** антивирусного сканирования ресурсов сервера как по команде администратора, так и по расписанию, заключающегося в однократной полной или выборочной проверке на наличие угроз объектов;

**2.4.10.3** помещения найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа;

**2.4.10.4** автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;

**2.4.10.5** запуска задач по расписанию и/или сразу после загрузки операционной системы;

**2.4.10.6** настройки расписания сканирования с указанием параметров запуска.

**2.4.11** Управление программой должно осуществляться как непосредственно через конфигурационные файлы, так и через графический интерфейс, реализованный для операционных систем типа Linux. Система управления должна поддерживать возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, действий по отношению к вредоносным объектам различных типов.

**2.4.12** Администратор системы должен иметь возможность:

**2.4.12.1** Определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;

**2.4.12.2** определять типы проверяемых файлов, в том числе с использованием масок;

**2.4.12.3** задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения;

**2.4.12.4** управлять детализацией протоколов антивирусной проверки;

**2.4.12.5** просматривать информацию об используемом ключевом файле и его владельце;

**2.4.12.6** запускать периодическую проверку в приоритетном или в фоновом режиме;

## 2.5 Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows

**2.5.1** Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:

**2.5.1.1** Осуществление антивирусной защиты на серверах, включая защиту от руткит-технологий.

**2.5.2** Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.

**2.5.3** Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию, должна обеспечивать защиту серверов под управлением операционных систем:

**2.5.3.1** Microsoft Windows Server 2000;

**2.5.3.2** Microsoft Windows Server 2003;

**2.5.3.3** Microsoft Windows Server 2008.

**2.5.3.4** Microsoft Windows Server 2012

**2.5.4** Компоненты Системы должны устойчиво функционировать на серверах в условиях их минимальной и максимальной загрузки без существенного снижения производительности.

**2.5.5** Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.

**2.5.6** Антивирусное программное обеспечение должно по умолчанию иметь оптимальные настройки 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 администраторами Системы и пользователями в рамках имеющихся у них прав.

**2.5.7** Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением системы.

**2.5.8** В Системе должна быть реализована возможность выбора приоритета сканирования, а также остановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.

**2.5.9** Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.

**2.5.10** Система должна обеспечивать:

**2.5.10.1** поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;

**2.5.10.2** 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;

**2.5.10.3** блокировку опасных макросов VBA в реальном времени;

**2.5.10.4** защиту от вредоносных сценариев, загружаемых с веб-страниц;

**2.5.10.5** помещение найденных зараженных файлов в специальное место на жестком диске — «карантин»;

**2.5.10.6** автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;

**2.5.10.7** запуск задач по расписанию и/или сразу после загрузки операционной системы.

**2.5.11** Система защиты серверов под управлением семейства ОС Microsoft Windows должна обеспечивать реализацию следующих функциональных возможностей:

**2.5.11.1** проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов посредством:

**2.5.11.1.1** антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;

**2.5.11.1.2** проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.

**2.5.12** В Системе должна быть реализована самозащита для всех ее 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.

**2.6** Требования к программным средствам антивирусной защиты файловых серверов Novell NetWare

**2.6.1** Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.

**2.6.2** Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных файлов всех типов.

**2.6.3** Система, используя актуальную на момент проведения тендера версию, должна обеспечивать защиту ресурсов серверов под управлением сетевой операционной системы Novell NetWare версий 4.11, 4.2, 5.1, 6.0, 6.5

**2.6.3.1** Антивирусное программное обеспечение должно по умолчанию иметь оптимальные с точки зрения безопасности и производительности работы настройки. При этом в случае необходимости внесения изменений Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы в рамках имеющихся у них прав.

**2.6.3.2** Компоненты Системы должны устойчиво функционировать на серверах в условиях их минимальной и максимальной загрузки без существенного снижения производительности в том числе за счет порождения нескольких одновременно действующих процессов проверки.

**2.6.4** Компоненты Системы должны иметь возможность управления использованием ресурсов сервера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.

**2.6.5** В Системе должна быть реализована возможность выбора приоритета сканирования, а также остановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.

**2.6.6** Система должна обеспечивать:

**2.6.6.1** проведение антивирусной проверки томов сервера по заранее заданному расписанию или запросу администратора;

**2.6.6.2** проверку «на лету» файлов, загружаемых на сервер и с него;

**2.6.6.3** отключения от сервера станций, с которой исходят вирусные атаки;

**2.6.6.4** отсылки уведомлений станциям, с которых исходит вирусная атака;

**2.6.6.5** отображения настроенных и запущенных процессов сканирования с указанием их статуса;

**2.6.6.6** ведения протокола проверки и управления его детализацией;

**2.6.6.7** помещения найденных чистых, зараженных или подозрительных файлов в специальные транзитные каталоги;

**2.6.6.8** автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;

**2.6.6.9** запуск задач по расписанию и/или сразу после загрузки операционной системы.

**2.6.7** Управление программой осуществляется с помощью консоли, установленной либо непосредственно на сервере, либо на любой удаленной рабочей станции.

**2.6.8** Администратор системы должен иметь возможность:

**2.6.8.1** Редактирования текстов уведомлений станциям, с которых происходят вирусные атаки;

**2.6.8.2** Настройке параметров и типов проверки – в том числе в заданное администратором время или по истечению заданного времени;

**2.6.8.3** Временного отключения настроенных антивирусных проверок;

**2.6.8.4** Задания списка файлов, каталогов и томов подлежащих антивирусной проверке;

**2.6.8.5** определения типов проверяемых файлов, в том числе с использованием масок;

**2.6.8.6** задания различных действий по отношению к различным типам вредоносных объектов в случае их обнаружения.

**2.6.8.7** управления приоритетом процессов проверки в системе и контроля их проведения;

**2.6.8.8** управления детализацией протоколов антивирусной проверки;

**2.6.8.9** просмотра результатов антивирусной проверки;

**2.6.9** Конфигурационный файл должен быть общим для всех программ семейства и храниться в каталоге установки. Настройки режимов для разных программ должны задаваться в отдельных разделах конфигурационного файла.

**2.7** Требования к программным средствам антивирусной защиты файловых серверов UNIX

**2.7.1** Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.

**2.7.2** Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных файлов всех типов.

**2.7.3** Система, используя актуальную на момент проведения тендера версию, должна обеспечивать защиту ресурсов серверов, использующих Samba версий 3.0.x - 3.6.x, и функционирующих под управлением операционных систем:

**2.7.3.1** Linux, имеющих версию ядра версия ядра 2.4.x и выше, а также версию glibc2.2 и выше;

**2.7.3.2** FreeBSD версии 6.x и выше для платформы Intel x86 и amd64;

**2.7.3.3** Solaris версии 10 для платформы Intel x86 и amd64

**2.7.4** Интеграция Системы с Samba должна осуществляться с помощью модуля VFS (Virtual File System).

**2.7.5** В случае использования версий Samba, отличных от вышеперечисленных, либо Samba для 64-битных платформ семейства Linux должна существовать возможность компиляции модулей интеграции из исходных кодов.

**2.7.6** Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью универсального пакета для UNIX систем, независимого от типа и версии используемой операционной системы, репозитория или пакета рассчитанного на работу с используемым в ОС менеджером пакетов

**2.7.7** Установка и обновление Системы должны быть возможны как через средства командной строки, так и с помощью графического инсталлятора.

**2.7.8** Система установки системы должна включать возможность автоматической установки модулей, необходимых для установки необходимых компонентов.

**2.7.9** Компоненты Системы должны устойчиво функционировать на серверах в условиях их минимальной и максимальной загрузки без существенного снижения производительности.

**2.7.10** Компоненты системы должны иметь возможность управления использованием серверных ресурсов при выполнении сканирования файлового пространства.

**2.7.11** В Системе должна быть реализована возможность задания приоритета антивирусного сканирования.

**2.7.12** Система должна поддерживать возможность порождения нескольких одновременно действующих процессов проверки.

**2.7.13** Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы настройки. При этом, в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и

гибкого изменения настроек администраторами Системы и пользователем в рамках имеющихся у них прав.

**2.7.14** Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением заданных файловых областей.

**2.7.15** Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:

**2.7.15.1** поиск и удаление вирусов всех известных типов в файлах;

**2.7.15.2** антивирусного сканирования ресурсов сервера, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде администратора, так и по расписанию;

**2.7.15.3** антивирусной проверке «на лету» файлов, загружаемых как на сервер, так и с него;

**2.7.15.4** помещения найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа;

**2.7.15.5** автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;

**2.7.15.6** запуска задач по расписанию и/или сразу после загрузки операционной системы;

**2.7.15.7** настройки расписания сканирования с указанием параметров запуска.

**2.7.16** Управление программой должно осуществляться как с помощью веб-интерфейса, так и непосредственно через конфигурационные файлы. Система управления должна поддерживать возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, и действий по отношению к вредоносным объектам различных типов.

**2.7.17** Администратор системы должен иметь возможность:

**2.7.17.1** определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки;

**2.7.17.2** определять типы проверяемых файлов, в том числе с использованием масок;

**2.7.17.3** задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения.

**2.7.17.4** управлять детализацией протоколов антивирусной проверки;

**2.7.17.5** просматривать результаты антивирусной проверки;

**2.7.17.6** просматривать информацию об используемом ключевом файле и его владельце;

**2.7.17.7** запускать периодическую проверку в приоритетном или в фоновом режиме;

**2.7.17.8** использовать альтернативные языковые файлы.

### 2.8 Требования по комплектности поставке

**2.8.1** В состав Системы должны входить:

**2.8.1.1** программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания;

**2.8.1.2** программные средства защиты пользователей от нежелательных массовых почтовых рассылок – спама;

**2.8.1.3** программные средства централизованного управления, мониторинга и обновления;

**2.8.1.4** обновляемые базы данных сигнатур всевозможных вредоносных программ.

**2.8.2** Комплект поставки должен содержать:

**2.8.2.1** необходимый набор серийных номеров либо ключевых файлов;

**2.8.2.2** 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.

### 2.9 Требования по технической поддержке Системы

**2.9.1** Техническая поддержка должна предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет.

**2.9.2** Техническая поддержка должна включать возможность предоставления выделенного специалиста, доступного в режиме 5/8

**2.9.3** Техническая поддержка должна включать возможность проведения расследования компьютерных инцидентов

**2.9.4** Техническая поддержка должна обеспечивать возможность получения специалистами и пользователями Заказчика информационной помощи по установке Системы и ее компонентов, в том числе:

**2.9.4.1** ответов на вопросы, а также получение инструкций относительно процесса установки и применения программного обеспечения;

**2.9.4.2** ответов на вопросы о наличии проблем в работе программного обеспечения, а также помощи в определение того, является ли данная проблема результатом сбоя программного обеспечения, ошибок настройки или же она вызвана проблемами, связанными с внешними условиями существования или установкой программного обеспечения.

**2.9.5** Web-сайт производителя Системы должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов производителя.

**Требования к качеству товара.**
Качество поставляемого товара должно соответствовать действующим стандартам и указанным характеристикам.