Приложение №2

к извещению о проведении запроса котировок

Приложение №2

к муниципальному контракту

№ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_ 2011г.

Технические требования к средствам антивирусной защиты

Оглавление

[Технические требования к создаваемой системе антивирусной защиты 1](#_Toc308434155)

[Общие требования 2](#_Toc308434156)

[Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows 2](#_Toc308434157)

[Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows 4](#_Toc308434158)

[Требования к программным средствам антивирусной защиты серверов масштаба предприятия под управлением ОС семейства Microsoft Windows и терминальных серверов 6](#_Toc308434159)

[Требования к программным средствам антивирусной защиты смартфонов 9](#_Toc308434160)

[Требования к системе управления антивирусной защитой 9](#_Toc308434161)

[Требования к обновлению антивирусных баз 13](#_Toc308434162)

[Требования к эксплуатационной документации 13](#_Toc308434163)

[Требования к технической поддержке 13](#_Toc308434164)

# Общие требования

Средства антивирусной защиты, предназначенные для развертывания в государственных организациях, должны быть 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 4 и требованиям технических условий.

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

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

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

Антивирусные средства должны включать:

* программные средства антивирусной защиты рабочих станций и серверов;
* программные средства антивирусной защиты мобильных устройств (смартфонов);
* программные средства централизованного управления, мониторинга и обновления;
* обновляемые базы данных сигнатур вредоносных программ и атак;
* эксплуатационную документацию на русском языке.

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

Программные средства антивирусной защиты систем рабочих станций под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:

* Microsoft® Windows® Embedded Standard 7 (Service Pack 1);
* Microsoft® Windows® Embedded POSReady 2009;
* Microsoft® Windows® Embedded POSReady 7;
* Microsoft Windows 2000 Professional (Service Pack 4 Rollup1);
* Microsoft Windows XP Professional (Service Pack 2 или выше);
* Microsoft Windows XP Professional x64 Edition (Service Pack 2 или выше);
* Microsoft Windows Vista Business/Enterprise/Ultimate (Service Pack 1 или выше);
* Microsoft Windows Vista Business/Enterprise/Ultimate x64 (Service Pack 1 или выше);
* Microsoft Windows 7 Professional/Enterprise/Ultimate;
* Microsoft Windows 7 Professional/Enterprise/Ultimate x64.

Программные средства антивирусной защиты систем рабочих станций под управлением семейства ОС Microsoft Windows должны обеспечивать 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;
* антивирусную проверку и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.;
* антивирусную проверку 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;
* защиту электронной корреспонденции, как от вредоносных программ, так и от спама. Проверку трафика на следующих протоколах:
* IMAP, SMTP, POP3, независимо от используемого почтового клиента;
* NNTP (только проверка на вирусы), независимо от почтового клиента;
* Независимо от типа протокола (в том числе MAPI, HTTP) в рамках работы плагинов, встроенных в почтовые программы Microsoft Office Outlook и The Bat!;
* Защиту HTTP-трафика - проверку всех объектов, поступающих на компьютер пользователя по протоколу HTTP, FTP;
* Проверку скриптов - 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;
* проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет-пейджерами;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* защиту от еще не известных вредоносных программ на основе анализа их поведения и контроле 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;
* защиту 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, включая беспроводные;
* проверка протокола IPv6;
* защиту от программ-маскировщиков, программ автодозвона на платные сайты, блокировку баннеров, всплывающих окон, вредоносных сценариев, загружаемых с Web-страниц и распознавание фишинг-сайтов;
* наличие компонента дающего возможность создания специальных правил запрещающих установку/запуск программ, компонент должен контролировать приложения по пути нахождения программы, метаданным, MD5 контрольной сумме;
* осуществлять контроль работы пользователя с внешними устройствами ввода / вывода, позволяя ограничивать доступ 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;
* блокирование функции автозапуска;
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* запускать специальную задачу для обнаружения уязвимостей в приложениях, установленных на компьютере пользователя, с возможностью предоставления отчета по обнаруженным уязвимостям;
* интеграция с системой обновления Windows Update, для установки патчей закрывающие обнаруженные уязвимости;
* гибкого управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* настройки проверки критических областей компьютера в качестве отдельной задачи;
* технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
* возможность устанавливать не все, а только выбранные компоненты антивирусной защиты;
* централизованно управляться с помощью единой системы управления.

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

Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:

* Windows 2000 Server/Advanced Server (Service Pack 4 Rollup1);
* Windows Server 2003 Standard/Enterprise (Service Pack 2);
* Windows Server 2003 x64 Standard/Enterprise (Service Pack 2);
* Windows Server 2003 R2 Standard/Enterprise Edition (Service Pack 2);
* Windows Server 2003 R2 x64 Standard/Enterprise Edition (Service Pack 2);
* Windows Server 2008 Standard/Enterprise (Service Pack 1 или выше);
* Windows Server 2008 x64 Standard/Enterprise (Service Pack 1 или выше);
* Windows Server 2008 R2 x64 Standard/Enterprise.

Программные средства антивирусной защиты файловых систем серверов под управлением семейства ОС Microsoft Windows должны обеспечивать 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;
* защиту 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;
* антивирусную проверку и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.;
* антивирусную проверку 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;
* защиту 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;
* наличием 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, защита 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;
* централизованно управляться с помощью единой системы управления.

# Требования к программным средствам антивирусной защиты серверов масштаба предприятия под управлением ОС семейства Microsoft Windows и терминальных серверов

Программные средства антивирусной защиты серверов масштаба предприятия под управлением семейства ОС Microsoft Windows и терминальных серверов должны функционировать на следующих версиях ОС:

* 32-битные платформы:
* Microsoft Windows 2000 Server с накопительным пакетом обновлений 1 к пакету обновлений 4 (Service Pack 4 + Rollup 1);
* Microsoft Windows 2000 Advanced Server с накопительным пакетом обновлений 1 к пакету обновлений 4 (Service Pack 4 + Rollup 1);
* 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 2000 Server;
* Microsoft Terminal на базе Windows 2003 Server;
* Microsoft Terminal на базе Windows Server 2008.

Программные средства антивирусной защиты серверов масштаба предприятия под управлением семейства ОС Microsoft Windows и терминальных серверов 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;
* Определение в объектах файловой системы сервера угрозы следующих типов:
* Классических вирусов;
* Сетевых червей;
* Троянских программ;
* Прочих вредоносных программ;
* Программ-реклам;
* Программ порнографического содержания;
* Потенциально опасных приложений.
* 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;
* Изоляцию зараженных компьютеров путем запрета пользователю зараженной рабочей станции обращаться к ресурсам сервера в течение определенного времени, что позволяет выявить источник заражения и провести лечение;
* 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 Active Scripting). 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) и Microsoft Operations Manager (МОМ);
* Cовместимость с системами управления дисковым пространством (Hierarchical Storage Management), позволяющая настраивать способы проверки для Offline Files;
* Оптимизация для использования на многопроцессорных серверах на базе технологии Intel Xeon™, 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 должны функционировать под управлением мобильных ОС:

* Symbian OS 9.1, 9.2, 9.3 Series 60 3rd (мобильные устройства Nokia);
* Microsoft Windows Mobile 5.0, 6.0, 6.1, 6.5;
* Android OS 1.5, 1.6, 2.0, 2.1, 2.2, 2.3.

Программные средства для антивирусной защиты смартфонов должны обеспечивать следующую функциональность:

* постоянную защитуфайловой системы смартфона, 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.
* проверку объектовфайловой системы, находящихся на смартфоне или на подключенных картах расширения памяти, по требованию пользователя и по расписанию;
* надежное изолирование зараженных объектовв 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;
* осуществлять функцию «антивор», т.е. обеспечивать блокировку мобильного устройства, удаление данных, сообщений и книги контактов, получение координат местоположения, а также определение, у кого находится пропавшее устройство.

# Требования к системе управления антивирусной защитой

Программные средства управления для всех защищаемых ресурсов, реализованных на платформах ОС Microsoft Windows и мобильных устройств на платформе Microsoft Windows Mobile и Symbian должны функционировать на следующих операционных системах:

Сервер администрирования:

* Microsoft Windows 2000 Server / Professional SP4 и выше (только 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 7 Professional/Enterprise/Ultimate (x32/x64).

Сервером администрирования должна использоваться одна из следующих СУБД:

* Microsoft SQL Server 2008;
* Microsoft SQL Server 2008 Express;
* Microsoft SQL Server 2005 SP2 или выше;
* Microsoft SQL Server 2005 Express Edition SP2 или выше;
* MySQL Enterprise 5.0.60 SP1, 5.0.70, 5.0.82 SP1;
* MySQL 5.0.67, 5.0.85;
* Microsoft SQL Server 2000 SP 3 и выше;
* Microsoft SQL Server 2000 Desktop Engine (MSDE) SP3 и выше.

Консоль администрирования:

* Microsoft Windows XP Professional SP2 и выше;
* Microsoft Windows XP Home Edition 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 x64 SP1 и всеми текущими обновлениями;
* Microsoft Windows Server 2008 R2;
* Microsoft Windows 7 Professional/Enterprise/Ultimate (x32/x64).

Агент администрирования:

* Microsoft Windows 2000 SP4;
* 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 7 Professional/Enterprise/Ultimate (x32/x64).

Программные средства управления для всех защищаемых ресурсов, реализованных на платформах ОС Microsoft Windows и мобильных устройств на платформе Microsoft Windows Mobile и Symbian 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;
* централизованную установку/обновление/удаление программных средств антивирусной защиты, настройку, администрирование, просмотр отчетов и статистической информации по их работе;
* централизованное удаление несовместимых приложений;
* централизованное управление установкой/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: удаленный - RPC, GPO, login script, агент администрирования, локальный -  автономный пакет установки;
* удаленная установка программных средств антивирусной защиты с последней версией баз приложения;
* автоматизированное обновление программных средств антивирусной защиты и антивирусных баз (для защищаемых ресурсов на базе ОС Microsoft Windows);
* автоматизированный поиск уязвимостей, в установленных приложения и операционной системе, на компьютерах пользователей, с возможностью предоставления отчета по обнаруженным уязвимостям и интеграцией с системой обновления Windows Update, для установки патчей закрывающие обнаруженные уязвимости;
* 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;
* централизованно осуществлять контроль работы пользователя с внешними устройствами ввода / вывода, позволяя ограничивать доступ 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;
* централизованный сбор информации о всех установленных на клиентских компьютерах приложениях;
* интеграция с CISCO NAC и MS NAP
* экспорта 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 должны обеспечивать 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.