

Общие требования

Антивирусные средства должны включать:

- Программные средства антивирусной защиты для рабочих станций Windows.
- Программные средства антивирусной защиты для рабочих станций MacOS.
- 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 мобильных устройств (смартфонов и планшетов).
- 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, должен быть на русском и английском языке.

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

Требования к программным средствам антивирусной защиты для рабочих станций Windows

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

- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

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

- Антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализация действий активного заражения;
- анализ поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
- анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокирование действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- возможность совершить откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- возможность ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений. Динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE в том числе и защищенных паролем;
- защита электронной почты от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP;
- фильтр почтовых вложений с возможностью переименования или удаления заданных типов файлов;
- Проверка трафика, поступающего на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
- блокировка баннеров и всплывающих окон на загружаемых Web-страницах;
- распознавание и блокировка фишинговых и небезопасных сайтов;
- наличие встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;

- контроль сетевых соединений, устанавливаемых с помощью сетевых мостов, с возможностью блокировки одновременной установки нескольких сетевых соединений.
- Наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп). Компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме MD5 или SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения. Компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
- осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
- возможность записи в журнал событий о записи и/или удалении файлов на съемных дисках;
- осуществление контроля работы пользователя с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
- наличие механизмов защиты от атак типа BadUSB;
- запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- Полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On. Наличие инструментов восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС. Должна быть реализована поддержка UEFI-систем;
- поддержка двухфакторной аутентификации при полнодисковом шифровании;
- шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению). Наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы в не защищенного периметра с помощью пароля;
- шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации.
- Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
- возможность установки только выбранных компонентов программного средства антивирусной защиты;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- возможность проверки целостности антивирусной программы;
- возможность добавления исключений из антивирусной проверки по хеш сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
- наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
- наличие защищенного хранилища для отчетов о работе антивируса;
- возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей;

Требования к программным средствам антивирусной защиты для рабочих станций Mac

Программные средства антивирусной защиты для рабочих станций Mac должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- macOS High Sierra 10.13
- macOS Sierra 10.12
- Mac OS X 10.11 (El Capitan)
- Mac OS X 10.10 (Yosemite)
- Mac OS X 10.9 (Mavericks)

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

- Резидентный антивирусный мониторинг;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- автоматическое обновление антивирусных баз по расписанию;
- резервное копирование зараженных файлов перед их удалением, для возможности восстановления;
- эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
- защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
- блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
- защита информации, передаваемой через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик);
- ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления, с возможностью управлять шифрованием FileVault.

Требования к программным средствам антивирусной защиты для рабочих станций Linux

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

- Ubuntu 14.04.5, 16.04.4, 17.10.1 LTS
- Red Hat Enterprise Linux 6.9, 7.4
- CentOS-6.9, 7.4
- Debian GNU / Linux 8.10, 9.4
- OracleLinux 7.4
- SUSE Linux Enterprise Server 12 SP3
- openSUSE 42.3

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

- Резидентный антивирусный мониторинг;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- проверка ресурсов доступных по SMB / NFS;
- эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj;
- проверка сообщений электронной почты в текстовом формате (Plain text);
- наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
- защита файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
- помещение подозрительных и поврежденных объектов на карантин;
- проверка почтовых баз приложений Microsoft Outlook
- возможность перехвата и проверки файловых операций на уровне SAMBA;
- управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
- 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 пользовательский графический интерфейс без root прав;

- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты для файловых серверов Windows

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

- Windows Server 2003, 2003 R2
- Windows Server 2008, 2008 R2
- Windows Server 2012, 2012 R2
- Windows Server 2016

Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

- Антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: Серверов терминалов и принт-серверов; Серверов приложений и контроллеров доменов; Файловых серверов;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем;
- защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
- 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 автоматическое запрещение выполнения тех из них, которые признаются опасными. Анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- Возможность проверки контейнеров Microsoft Windows.
- Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
- защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов. Перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления.
- Наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory и локальных пользователей/групп). Компонент должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме MD5 или SHA256. Компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки. Также компонент должен иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
- осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
- осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем.;
- Информирование администратора о подключении внешних устройств.
- Механизмы защиты от эксплуатирования уязвимостей в памяти процессов с помощью техник снижения рисков;
- ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
- 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);

- ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
- возможность интеграции с SIEM системами;
- Наличие механизмов автоматической генерации правил для контроля устройств и приложений;
- возможность указания количества рабочих процессов антивируса в ручную;
- возможность отключить графический интерфейс;
- наличие удаленной и локальной консоли управления;
- управления параметрами антивируса из командной строки;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;

Требования к программным средствам антивирусной защиты для файловых серверов Linux

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

- Ubuntu 14.04.5, 16.04.4, 17.10.1, 18.04. LTS
- Red Hat® Enterprise Linux® 6.9, 7.4
- CentOS-6.9, 7.4
- Debian GNU/Linux 8.10, 9.4
- OracleLinux 7.4.
- SUSE® Linux Enterprise Server 12 SP3.
- openSUSE® 42.3.

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

- Резидентный антивирусный мониторинг;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- проверка ресурсов доступных по SMB / NFS;
- эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj.;
- проверка сообщений электронной почты в текстовом формате (Plain text);
- наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
- защита файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
- помещение подозрительных и поврежденных объектов на карантин;
- проверка почтовых баз приложений Microsoft Outlook
- возможность перехвата и проверки файловых операций на уровне SAMBA;
- управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
- 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 пользовательский графический интерфейс без root прав;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Требования к программным средствам антивирусной защиты мобильных устройств

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

- Android 4.2– 9.0;
- Apple iOS 9.0 – 11.4.1;

Программные средства для антивирусной защиты смартфонов для ОС Android должны обеспечивать следующую функциональность:

- Постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки на репутационных облачных сервисах производителя антивирусных средств защиты;
- проверка файловой системы устройства по требованию и по расписанию;
- Мгновенная проверка устанавливаемых приложений
- Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты. Поддержка белых списков разрешенных сайтов;
- наличие хранилища для изолирования зараженных объектов;
- обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;
- блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений. Поддержка белых списков разрешенных приложений;
- блокировка системных приложений;
- возможность получения политик безопасности через Google Cloud Messaging;
- базовая поддержка Android for Work;
- наличие возможности создания специальной оболочки для мобильных программ с целью контроля действий программы, возможностью удаления данных и настроек программы, добавления дополнительного пароля для старта приложения, в том числе с помощью учетных данных Active Directory ;
- возможность заблокировать wi-fi и bluetooth модули, а так же использование камеры мобильного устройства;
- указание параметров подключения к wi-fi сетям;
- наличие возможности указания обязательных к установке приложений;
- блокирование нежелательных SMS сообщений;
- возможность блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);
- постоянная проверка телефона на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
- возможность получения текущего номера SIM-карты телефона посредством CMC, возможность автоматической блокировки устройства при смене SIM-карты или при включении телефона без SIM-карты;
- поддержка технологий Samsung KNOX1 и KNOX2.

Программные средства для антивирусной защиты смартфонов для ОС Apple iOS должны обеспечивать следующую функциональность:

- Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
- возможность определения местоположения устройства.

Программные средства для антивирусной защиты смартфонов для ОС Windows Phone должны обеспечивать следующую функциональность:

- Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
- возможность определения местоположения устройства.

Решение должно централизованно управлять с помощью единой консоли управления.

Требования к программным средствам централизованного управления, мониторинга и обновления

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

- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10
- Windows Server 2008, 2008 R2
- Windows Server 2012, 2012 R2
- Windows Server 2016

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

- Microsoft SQL
- MySQL

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:

- Установка системы управления антивирусной защиты из единого дистрибутива.
 - Выбор установки в зависимости от количества защищаемых узлов.
 - Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации.
 - Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети.
 - Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD.
 - Централизованные установка, обновление и удаление программных средств антивирусной защиты.
- Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе.
- Централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления.
 - Сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
 - Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки.
 - Возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от УЗ, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности. Должна быть реализована возможность поддержки иерархии таких триггеров.
 - Автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей.
 - Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка 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.
 - Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне.
 - Наличие преднастроенных ролей пользователей средств централизованного управления. Должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей.
 - Создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня.
 - Поддержка мультиарендности (multi-tenancy) для серверов управления.
 - 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.
 - Инвентаризация установленного ПО и оборудования на компьютерах пользователей.
 - Возможность подключения по RDP или штатными средствами из консоли управления. Пользователю должен выводиться запрос на разрешение дистанционного подключения.
 - Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них.
 - Наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal). Должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ. Возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС.
 - Возможность импортировать образ операционной системы из дистрибутивов (WIM)
 - Наличие системы контроля лицензий стороннего ПО с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии.
 - Автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др) и автоматическая централизованная установка этих пакетов приложений на компьютеры
 - Функция управления мобильными устройствами через сервер Exchange ActiveSync.
 - Функция управления мобильными устройствами через сервер iOS MDM.
 - Возможность отправки SMS-оповещений о заданных событиях.
 - Централизованная установка приложений на управляемые мобильные устройства.
 - Централизованная установка сертификатов на управляемые мобильные устройства.
 - Поддержка функциональности управления шифрованием данных.

- Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления.
- Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления.
- Построение графических отчетов как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и тд.
- Наличие преднастроенных стандартных отчетов о работе системы.
- Экспорт отчетов в файлы форматов PDF и XML.
- Централизованное управление объектами резервных хранилищ и карантин по всем ресурсам сети, на которых установлено антивирусное программное обеспечение.
- Создание внутренних учетных записей для аутентификации на сервере управления.
- Создание резервной копии системы управления встроенными средствами системы управления.
- Поддержка Windows Failover Clustering.
- Поддержка интеграции с Windows сервисом Certificate Authority.
- Наличие веб-консоли управления приложением.
- Наличие портала самообслуживания пользователей. Портал самообслуживания должен обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя.
- 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.
- 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 по телефону, электронной почте и через Интернет.
- Web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов.