Утверждаю

\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ ФИО

# ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Предмет закупки:

Передача права на использование

Kaspersky Embedded System Security -5000+Node 1 year Base License

для АКБ «Микрокредитбанк»

Ташкент

2025

Оглавление

[ТЕХНИЧЕСКОЕ ЗАДАНИЕ 1](#_Toc200542904)

[Наименование и спецификация предмета закупки 3](#_Toc200542905)

[Общие требования к поставщику 3](#_Toc200542906)

[Общие требования к продукту 3](#_Toc200542907)

[Требования к программным средствам антивирусной защиты для банкоматов и терминалов оплаты 3](#_Toc200542908)

[Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows 6](#_Toc200542909)

[Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux 9](#_Toc200542910)

[Требования к обновлению антивирусных баз 11](#_Toc200542911)

[Требования к эксплуатационной документации 12](#_Toc200542912)

[Требования к технической поддержке 12](#_Toc200542913)

# Наименование и спецификация предмета закупки

|  |  |  |
| --- | --- | --- |
| Артикул | Наименование | Количество |
| KL48912AYFS | Передача права на использование Kaspersky Embedded System Security -5000+Node 1 year Base License | 150 |

# Общие требования к поставщику

* Опыт аналогичных поставок не менее 3 лет.
* Наличие действующего партнерского сертификата не ниже уровня «Silver».
* Не менее двух сертифицированных инженеров, наличие сертификатов обязательно.

# Общие требования к продукту

Антивирусные средства должны включать:

* программные средства антивирусной защиты для банкоматов и терминалов оплаты;
* 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 банкоматов и терминалов оплаты

Программные средства антивирусной защиты для защиты банкоматов и терминалов оплаты должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий Windows:

* Рабочие станции:
  + Windows XP Professional SP2 32-разрядная / 64-разрядная.
  + Windows XP Professional SP3 32-разрядная.
  + Windows 7 Home / Professional / Enterprise / Ultimate SP1 32-разрядная / 64-разрядная.
  + Windows 8 Pro / Enterprise 32-разрядная / 64-разрядная.
  + Windows 8.1 Pro / Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 версии 1507 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 LTSC 2015 версии 1507 32-разрядная / 64-разрядная.
  + Windows 10 RS1 версии 1607 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 LTSC 2016 версии 1607 32-разрядная / 64-разрядная.
  + Windows 10 RS2 версии 1703 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 RS3 версии 1709 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 RS4 версии 1803 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 RS5 версии 1809 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 LTSC 2019 версии 1809 32-разрядная / 64-разрядная.
  + Windows 10 19H2 версии 1909 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 21H2 версии 21H2 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 LTSC 2021 версии 21H2 32-разрядная / 64-разрядная.
  + Windows 10 22H2 версии 22H2 Home / Pro / Education / Enterprise 32-разрядная / 64-разрядная.
  + Windows 11 21H2 версии 21H2 Home / Pro / Education / Enterprise 64-разрядная.
  + Windows 11 22H2 версии 22H2 Home / Pro / Education / Enterprise 64-разрядная.
  + Windows 11 23H2 версии 23H2 Home / Pro / Education / Enterprise 64-разрядная.
  + Windows 11 24H2 версия 24H2 Home / Pro / Education / Enterprise 64-разрядная.
* Серверы:
  + Windows Server 2003 SP2 Standard / Enterprise 32-разрядная / 64-разрядная.
  + Windows Server 2003 R2 SP2 Standard / Enterprise 32-разрядная / 64-разрядная.
  + Windows Server 2008 SP2 Standard / Enterprise 32-разрядная / 64-разрядная.
  + Windows Server 2008 R2 SP1 Standard / Enterprise 64-разрядная.
* Встраиваемые системы:
  + Windows XP Embedded SP2 (WEPOS) 32-разрядная / 64-разрядная.
  + Windows XP Embedded SP3 (POS Ready 2009) 32-разрядная.
  + Windows 7 Embedded SP1 (POSReady 7) 32-разрядная / 64-разрядная.
  + Windows 8.0 Embedded Industry Pro 32-разрядная / 64-разрядная.
  + Windows 8.1 Embedded Industry Pro 32-разрядная / 64-разрядная.
  + Windows 10 версии 1507 IoT Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 версии 1607 IoT Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 версии 1703 IoT Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 версии 1709 IoT Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 версии 1803 IoT Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 версии 1809 IoT Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 версии 1909 IoT Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 версии 21H2 IoT Enterprise 32-разрядная / 64-разрядная.
  + Windows 10 версии 22H2 IoT Enterprise 32-разрядная / 64-разрядная.
  + Windows 11 версии 21H2 IoT Enterprise 64-разрядная.
  + Windows 11 версии 22H2 IoT Enterprise 64-разрядная.
  + Windows 11 версии 23H2 IoT Enterprise 64-разрядная.
  + Windows 11 версии 24H2 IoT Enterprise 64-разрядная.

Программные средства антивирусной защиты для защиты банкоматов и терминалов оплаты должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий Linux:

Поддерживаемые 32-битные операционные системы:

* Debian GNU/Linux 11.0 и выше.
* Debian GNU/Linux 12.0 и выше.

Поддерживаемые 64-битные операционные системы:

* AlmaLinux OS 9.0 и выше.
* AlterOS 7.5 и выше.
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8).
* CentOS Stream 9.
* Debian GNU/Linux 11.0 и выше.
* Debian GNU/Linux 12.0 и выше.
* EMIAS 1.0 и выше.
* EulerOS 2.0 SP10.
* Oracle Linux 9.0 и выше.
* Red Hat Enterprise Linux 8.0 и выше.
* Red Hat Enterprise Linux 9.0 и выше.
* Rocky Linux 9.0 и выше.
* SUSE Linux Enterprise Server 15 и выше.
* Ubuntu 20.04 LTS.
* Ubuntu 22.04 LTS.
* Ubuntu 24.04 LTS.
* Альт СП Рабочая Станция релиз 10.
* Альт СП Сервер релиз 10.
* РЕД ОС 7.3.
* РЕД ОС 8.0.
* РОСА "Кобальт" 7.9 Рабочая станция.
* РОСА "Кобальт" 7.9 Сервер.

РОСА "Хром" 12 Рабочая станция.Программные средства антивирусной защиты для банкоматов и терминалов оплаты должны обеспечивать реализацию следующих функциональных возможностей:

* антивирусное сканирование в режиме реального времени и по расписанию;
* автоматическое антивирусное сканирование подключаемых USB-накопителей с возможностью настройки параметров сканирования;
* эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* антивирусная проверка и лечение файлов в архивах;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* настраиваемый список исключений и доверенных процессов;
* механизмы оптимизации проверки и работы антивирусного модуля за счет технологии кеширования информации о проверяемых файлах;
* защита процессов от попыток эксплуатации уязвимостей в оперативной памяти системы, с режимом прерывания процесса и режимом информирования;
* задание правил блокировки недоверенных исполняемых файлов, скриптов и MSI-пакетов, в том числе в виде создание белого списка доверенных приложений;
* создание разрешающих и запрещающих правил запуска приложений на основании хэш-суммы, сертификата и пути нахождения приложения;
* блокировка запуска не доверенных DLL;
* автоматическое создание белого списка приложений на основе результатов сканирования действующего банкомата или терминала оплаты;
* работа модуля контроля приложений должна предоставлять возможность работы в тестовом режиме, без активной блокировки не доверенных приложений. Система должна только оповещать о событиях запуска таких приложений;
* возможность установки и работы продукта без антивирусных баз;
* механизм автоматического обновления белого списка программного обеспечения во время обновления сторонних программ на устройстве;
* блокировка недоверенных USB-накопителей и CD\DVD устройств. Должна быть реализована возможность ведения списка доверенных устройств;
* контроль подключения сетевых карт и модемов;
* автоматическое создание списка доверенных устройств на основании сканирования действующего банкомата или терминала оплаты;
* запуск антивируса в безопасном режиме операционной системы;
* интеграция с сетевым экраном Microsoft Windows с возможностью создания правил;
* 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;
* защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* управление с помощью локальной или удаленной консоли;
* управление с помощью командной строки;
* возможность отложенного запуска службы при старте операционной системы;
* блокировка USB-подключаемых устройств с поддержкой технологии UAS;
* возможность включить или выключить защиту файлов и ключей реестра продукта от внешних угроз;
* возможность запретить запуск приложений, за исключением приложений, подписанных доверенными подписями.

# Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows

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

* Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.
* Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSB) 64-разрядная.
* Windows Server 2019 Standard/Datacenter/Core 64-разрядная.
* Windows Server 2022 Standard/Datacenter/Core 64-разрядная.
* Windows Storage Server 2019 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

* VMware vSphere 6.7.
* VMware vSphere 7.0.
* Citrix XenServer 7.1 LTSR.
* Citrix XenServer 8.x.
* Parallels Desktop 18.
* Oracle VM VirtualBox 7.x.

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

* Microsoft SQL Server 2016 (все редакции) 64-разрядная.
* Microsoft SQL Server 2017 (все редакции) для Windows/Linux 64-разрядная.
* Microsoft SQL Server 2019 (все редакции) для Windows/Linux 64-разрядная (требуются дополнительные действия).
* Microsoft SQL Server 2022 (все редакции) для Windows/Linux 64-разрядная.
* MySQL 5.7 Community 32-разрядная/64-разрядная.
* MySQL 8.0 Community 32-разрядная/64-разрядная.
* MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.
* MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
* PostgreSQL 13.x 64-разрядная.
* PostgreSQL 14.х 64-разрядная.
* PostgreSQL 15.x 64-разрядная.
* Postgres Pro 13.x Windows/Linux 64-разрядная.
* Postgres Pro 14.x Windows/Linux 64-разрядная.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
* 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 работе средств защиты;
* 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;
* указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* иерархии триггеров, по которым происходит перераспределение;
* 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 прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* 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;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* функция управления мобильными устройствами через сервер iOS MDM;
* отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства;
* указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* 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 по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* поддержка Windows Failover Clustering;
* поддержка интеграции с Windows сервисом Certificate Authority;
* наличие портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
* интеграции по OpenAPI;
* управления антивирусной защитой с использованием WEB консоли;
* возможность интеграции с SIEM системами и передача событий в форматах Syslog, CEF, LEEF;
* двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
* использования дополнительной аутентификация после изменения параметров учетной записи пользователя.
* возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами;
* возможность развернуть сервер администрирования как систему высокой доступности;
* удаленная диагностика клиентских устройств на базе Windows и Linux (получение трассировок, журналов событий, дампов, остановка и запуск приложений);
* возможность отозвать права локального администратора учетных записей на управляемых устройствах с операционной системой Linux;
* возможность изменить пароль локальной учетной записи на управляемых устройствах с операционной системой Linux.

# Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux

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

* Debian GNU/Linux 11.х (Bullseye) 64-разрядная.
* Debian GNU/Linux 12 (Bookworm) 64-разрядная.
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная.
* Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
* CentOS Stream 9 64-разрядная.
* Red Hat Enterprise Linux Server 7.x 64-разрядная.
* Red Hat Enterprise Linux Server 8.x 64-разрядная.
* Red Hat Enterprise Linux Server 9.x 64-разрядная.
* SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная.
* SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная.
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная.
* Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядная.
* Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядная.
* Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядная.
* Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
* Альт СП Сервер 10 64-разрядная.
* Альт Сервер 10 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная.
* Альт СП Рабочая станция 10 64-разрядная.
* Альт Рабочая станция 10 64-разрядная.
* Oracle Linux 7 64-разрядная.
* Oracle Linux 8 64-разрядная.
* Oracle Linux 9 64-разрядная.
* Platform V SberLinux OS Server (SLO) 8.8 64-разрядная.
* РЕД ОС 7.3 Сервер 64-разрядная.
* РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
* РЕД ОС 8 Сертифицированная редакция 64-разрядная.
* РОСА "КОБАЛЬТ" 7.9 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

* VMware vSphere 6.7.0.
* VMware vSphere 7.0.3.
* Citrix XenServer 7.x.
* Citrix XenServer 8.2.
* Parallels Desktop 18.
* Oracle VM VirtualBox 7.0.12.
* Kernel-based Virtual Machine (все поддерживаемые ОС Linux).

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

* MySQL 5.7 Community 32-разрядная/64-разрядная.
* MySQL 8.0 32-разрядная/64-разрядная.
* MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.4 (сборка 10.4.20 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.6 (сборка 10.6.9 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.11 (сборка 10.11.3 и выше) 32-разрядная/64-разрядная.
* MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
* PostgreSQL 13.х 64-разрядная.
* PostgreSQL 14.х 64-разрядная.
* PostgreSQL 15.х 64-разрядная.
* Postgres Pro 13.х (все редакции) 64-разрядная.
* Postgres Pro 14.х (все редакции) 64-разрядная.
* Postgres Pro 15.х (все редакции) 64-разрядная.
* Platform V Pangolin 5.4.0 64-разрядная.
* Jatoba 4 64-разрядная.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* иерархии триггеров, по которым происходит перераспределение;
* 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 прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* 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;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* наличие системы контроля возникновения вирусных эпидемий;
* управления антивирусной защитой с использованием WEB консоли;
* обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;
* с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;
* использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули;
* выступать в качестве главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных.
* экспорт и импорт выборок событий;
* получение информации о программах, установленных на управляемые устройства;
* возможность поиска устройств по контроллерам доменов Microsoft Active Directory и Samba;
* возможность автоматизированного переноса данных с сервера администрирования под управлением ОС Windows на сервер администрирования под управлением ОС Linux;
* возможность удалённой диагностики управляемых устройств;
* поддержка кластерной технологии;
* возможность централизованного удаления несовместимого ПО с управляемых устройств.

# Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

* создания правил обновления 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 электронной почте и через Интернет;
* Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.