**ОПИСАНИЕ ОБЪЕКТА ЗАКУПКИ**

**Приобретение лицензий программного обеспечения для антивирусной защиты компьютеров и серверного оборудования**

1. Общие сведения
   1. Наименование оказываемых услуг

Приобретение лицензий программного обеспечения для антивирусной защиты компьютеров и серверного оборудования.

Код позиции по ОКПД2: 58.29.29.000 (Обеспечение программное прикладное прочее на электронном носителе).

Код позиции по КТРУ: 58.29.11.000-00000003 (Программное обеспечение).

* 1. Обязательные характеристики

Обязательные характеристики указаны в Таблице 1.

Таблица 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | Код позиции по КТРУ | Наименование | Кол-во | Наименование показателя | Содержание (значение) показателя | Единица измерения характеристики | Обоснование использования характеристик |
| 1 | 58.29.11.000-00000003 | Программное обеспечение | 5200 | Класс программ для электронных вычислительных машин и баз данных | (03.06) Средства антивирусной защиты | - | 58.29.11.000-00000003 |
| Способ предоставления | Экземпляр на материальном носителе | - | 58.29.11.000-00000003 |
| Копия электронного экземпляра | - | 58.29.11.000-00000003 |
| Вид лицензии | Простая (неисключительная) | - | 58.29.11.000-00000003 |
| 2 | 58.29.11.000-00000003 | Программное обеспечение | 400 | Класс программ для электронных вычислительных машин и баз данных | (03.06) Средства антивирусной защиты | - | 58.29.11.000-00000003 |
| Способ предоставления | Экземпляр на материальном носителе | - | 58.29.11.000-00000003 |
| Копия электронного экземпляра | - | 58.29.11.000-00000003 |
| Вид лицензии | Простая (неисключительная) | - | 58.29.11.000-00000003 |

* 1. **Место предоставления услуг**

Свердловская Область, г.о. город Екатеринбург, г Екатеринбург, ул Большакова, стр. 105 (государственное бюджетное учреждение Свердловской области «Оператор электронного правительства»).

* 1. **Сроки (периоды) предоставления услуг**

В течение 10 (десяти) рабочих дней со дня заключения Контракта.

* 1. **Срок действия лицензий**

Срок действия лицензий – 1 год с 04.06.2025.

1. **Общие требования**

Программное обеспечение для антивирусной защиты компьютеров и серверного оборудования должно поставляться совместно с эксплуатационной документацией (формуляр (паспорт) на программное изделие, сертификат (лицензионный сертификат), действующий Сертификат соответствия ФСТЭК России, действующий Сертификат соответствия ФСБ России) на русском языке.[[1]](#footnote-2)

Сертификат (лицензионный сертификат) на программное обеспечение для антивирусной защиты компьютеров и серверного оборудования должен быть свободен от любых прав третьих лиц, не находиться под запретом (арестом), в залоге и не являться предметом спора третьих лиц.

Антивирусные средства должны включать:

* Программные средства антивирусной защиты для рабочих станций Windows.
* Программные средства антивирусной защиты для рабочих станций Linux.
* Программные средства антивирусной защиты для рабочих станций Mac OS.
* Программные средства антивирусной защиты для файловых серверов Windows.
* Программные средства антивирусной защиты для файловых серверов Linux.
* Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows.
* Программные средства централизованного управления, мониторинга и обновления.
* Обновляемые базы данных сигнатур вредоносных программ и атак.

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.

Программное обеспечение должно обеспечивать защиту 5600 устройств (5200 шт. – продление прав на неисключительные лицензии для автоматизированных рабочих мест и серверов, 400 шт. – передача прав на неисключительные лицензии для автоматизированных рабочих мест и серверов).

Программное обеспечение должно иметь возможность интеграции с центром администрирования антивирусной защиты (Kaspersky Security Center 14), установленным в инфраструктуре Заказчика, а также обладать возможностью управления средствами данного центра администрирования.

1. **Требования к программным средствам антивирусной защиты для рабочих станций Windows**

Средства антивирусной защиты для рабочих станций Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. № 28 уполномоченным органом (ФСТЭК), по типу В и Г не ниже второго класса защиты.

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;
* Microsoft Windows 11.

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

* возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью;
* возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
* возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
* возможность читать информацию из записей аудита;
* ограничение доступа к чтению записей аудита;
* поиск, сортировка и упорядочение данных аудита;
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности;
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
* поддержка определенных ролей их ассоциации с конкретными администраторами безопасности или пользователями;
* возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;
* возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
* возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
* возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов, удаления кода из файлов и системных областей носителей информации;
* возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы;
* отображение сигнала тревоги об обнаружении зараженных файлов;
* возможность восстановления функциональных свойств зараженных объектов;
* возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса;
* возможность контроля доступа к веб-ресурсам;
* возможность контроля за запуском ПО на защищаемой рабочей станции или сервере.

Кроме того, программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

* 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;
* возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени для получения вердикта по запускаемой программе или файлу;
* антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* 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, c 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;
* возможность запуска специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
* 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.

1. **Требования к программным средствам антивирусной защиты для рабочих станций Linux**

Средства антивирусной защиты для рабочих станций Linux должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу В и Г не ниже второго класса защиты.

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

* Поддерживаемые 32-битные операционные системы:
  + Ubuntu 16.04 LTS;
  + Red Hat® Enterprise Linux® 6.7;
  + Red Hat Enterprise Linux 7.2;
  + CentOS-6.7;
  + Debian GNU / Linux 8.6;
  + Debian GNU / Linux 9.4;
  + Linux Mint 18.2;
  + Linux Mint 19;
  + Альт Линукс СПТ 7.0 (работа с графическим пользовательским интерфейсом не поддерживается);
  + Альт 8 СП Рабочая станция;
  + Альт 8 СП Сервер
  + Альт Линукс 8.2 Рабочая станция;
  + Альт Линукс 8.2 Рабочая станция К;
  + Альт Линукс 8.2 Сервер;
  + Альт Линукс 8.2 Образование;
  + Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6);
  + Лотос;
  + РЕД ОС.
* Поддерживаемые 64-битные операционные системы:
  + Ubuntu 16.04 LTS;
  + Ubuntu 18.04 LTS;
  + Red Hat Enterprise Linux 6.7;
  + Red Hat Enterprise Linux 7.2;
  + CentOS-6.7;
  + CentOS-7.2;
  + Debian GNU / Linux 8.6;
  + Debian GNU / Linux 9.4;
  + OracleLinux 7.3;
  + SUSE® Linux Enterprise Server 15;
  + openSUSE® 15;
  + Альт Линукс СПТ 7.0 (работа с графическим пользовательским интерфейсом не поддерживается);
  + Альт 8 СП Рабочая станция;
  + Альт 8 СП Сервер;
  + Альт Линукс 8.2 Рабочая станция;
  + Альт Линукс 8.2 Рабочая станция К;
  + Альт Линукс 8.2 Сервер;
  + Альт Линукс 8.2 Образование;
  + Amazon Linux AMI;
  + Linux Mint 18.2;
  + Linux Mint 19;
  + Micro Focus Open Enterprise Server 2018;
  + Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды);
  + Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды);
  + Astra Linux Common Edition 2.12;
  + Astra Linux SE 1.7.x Воронеж;
  + Astra Linux SE 1.8.x Воронеж;
  + программный комплекс терминального доступа «Циркон 36КТ»;
  + программный комплекс терминального доступа «Циркон 36CТ»;
  + ОС РОСА «КОБАЛЬТ» (версия 7.3 для клиентских систем);
  + ОС РОСА «КОБАЛЬТ» (версия 7.3 для серверных систем);
  + ЕМИАС 1.0;
  + Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6);
  + Лотос;
  + РЕД ОС.

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

* возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
* возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
* возможность читать информацию из записей аудита;
* ограничение доступа к чтению записей аудита;
* поиск, сортировка и упорядочение данных аудита;
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
* поддержка определенных ролей их ассоциации с конкретными администраторами безопасности и администраторами серверов или пользователями;
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности;
* возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;
* возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
* возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
* возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов, удаления кода из файлов и системных областей носителей информации;
* возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы;
* отображение сигнала тревоги об обнаружении вредоносного программного обеспечения;
* возможность восстановления функциональных свойств зараженных объектов;
* возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса.

Кроме того, программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

* резидентный антивирусный мониторинг;
* возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени 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;
* настройка возможности управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* возможность добавления точек монтирования в глобальные исключения;
* возможность отслеживать целостность указанных файлов в режиме мониторинга в реальном времени и в режиме проверки по требованию.

1. **Требования к программным средствам антивирусной защиты для рабочих станций Mac**

Средства антивирусной защиты для рабочих станций Mac должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты.

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

* macOS 10.13 High Sierra;
* macOS 10.12 Sierra;
* OS X 10.11 El Capitan;
* OS X 10.10 Yosemite;
* OS X 10.9 Mavericks.

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

* возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
* возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
* возможность читать информацию из записей аудита;
* ограничение доступа к чтению записей аудита;
* поиск, сортировка и упорядочение данных аудита;
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности;
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
* поддержка определенных ролей их ассоциации с конкретными администраторами безопасности, администраторами серверов и пользователями;
* возможность выполнять проверки с целью обнаружения зараженных объектов;
* возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
* возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
* возможность выполнять проверки с целью обнаружения зараженных объектов путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
* возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из зараженных объектов;
* возможность отображения сигнала тревоги на рабочей станции администратора безопасности;
* возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения.

Кроме того, программные средства антивирусной защиты для рабочих станций Mac должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

* резидентный антивирусный мониторинг;
* эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени для получения вердикта по запускаемой программе или файлу;
* 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 локальных репутационных облачных сервисов производителя антивирусных средств защиты;
* защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, HTTPS;
* автоматическое обновление антивирусных баз по расписанию;
* защита информации, передаваемой через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик);
* возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы.

1. **Требования к программным средствам антивирусной защиты для файловых серверов Windows**

Средства антивирусной защиты для файловых серверов Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты.

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

* Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1;
* Microsoft Windows Server 2008 Standard / Enterprise x86 Edition SP2;
* Microsoft Windows Server 2008 Standard / Enterprise x64 Edition SP2;
* Microsoft Windows Small Business Server 2011 Essentials / Standard x64 Edition;
* Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition;
* Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition;
* Microsoft Windows MultiPoint Server 2012 x64 Edition;
* Microsoft Windows Server 2016;
* Microsoft Windows Server 2019;
* Microsoft Windows Server 2022.

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

* возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью;
* возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
* возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
* возможность читать информацию из записей аудита;
* ограничение доступа к чтению записей аудита;
* поиск, сортировка и упорядочение данных аудита;
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности;
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
* поддержка определенных ролей их ассоциации с конкретными администраторами безопасности или пользователями;
* возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;
* возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
* возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
* возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов, удаления кода из файлов и системных областей носителей информации;
* возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы;
* отображение сигнала тревоги при обнаружении зараженных файлов;
* возможность восстановления функциональных свойств зараженных объектов;
* возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса;
* возможность контроля за запуском программного обеспечения на защищаемой рабочей станции или сервере.

Кроме того, программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

* антивирусное сканирование в режиме реального времени и по запросу;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени для получения вердикта по запускаемой программе или файлу;
* наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов, включая создание сетевых правил для конкретных программ;
* защита от сетевых атак с использованием правил сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
* возможность запуска специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
* антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* настройки проверки критических областей сервера в качестве отдельной задачи;
* возможность 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);
* 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;
* наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, а также обеспечивать возможность исключения из правил для определенных пользователей из Active Directory;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

1. **Требования к программным средствам антивирусной защиты для файловых серверов Linux**

Средства антивирусной защиты для файловых серверов Linux должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты.

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

* Поддерживаемые 32-битные операционные системы:
  + Ubuntu 16.04 LTS;
  + Red Hat® Enterprise Linux® 6.7;
  + Red Hat Enterprise Linux 7.2;
  + CentOS-6.7;
  + Debian GNU / Linux 8.6;
  + Debian GNU / Linux 9.4;
  + Linux Mint 18.2;
  + Linux Mint 19;
  + Альт Линукс СПТ 7.0 (работа с графическим пользовательским интерфейсом не поддерживается);
  + Альт 8 СП Рабочая станция;
  + Альт 8 СП Сервер
  + Альт Линукс 8.2 Рабочая станция;
  + Альт Линукс 8.2 Рабочая станция К;
  + Альт Линукс 8.2 Сервер;
  + Альт Линукс 8.2 Образование;
  + Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6);
  + Лотос;
  + РЕД ОС.
* Поддерживаемые 64-битные операционные системы:
  + Ubuntu 16.04 LTS;
  + Ubuntu 18.04 LTS;
  + Red Hat Enterprise Linux 6.7;
  + Red Hat Enterprise Linux 7.2;
  + CentOS-6.7;
  + CentOS-7.2;
  + Debian GNU / Linux 8.6;
  + Debian GNU / Linux 9.4;
  + OracleLinux 7.3;
  + SUSE® Linux Enterprise Server 15;
  + openSUSE® 15;
  + Альт Линукс СПТ 7.0 (работа с графическим пользовательским интерфейсом не поддерживается);
  + Альт 8 СП Рабочая станция;
  + Альт 8 СП Сервер;
  + Альт Линукс 8.2 Рабочая станция;
  + Альт Линукс 8.2 Рабочая станция К;
  + Альт Линукс 8.2 Сервер;
  + Альт Линукс 8.2 Образование;
  + Amazon Linux AMI;
  + Linux Mint 18.2;
  + Linux Mint 19;
  + Micro Focus Open Enterprise Server 2018;
  + Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды);
  + Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды);
  + Astra Linux Common Edition 2.12;
  + Astra Linux SE 1.7.x Воронеж;
  + Astra Linux SE 1.8.x Воронеж;
  + программный комплекс терминального доступа «Циркон 36КТ»;
  + программный комплекс терминального доступа «Циркон 36CТ»;
  + ОС РОСА «КОБАЛЬТ» (версия 7.3 для клиентских систем);
  + ОС РОСА «КОБАЛЬТ» (версия 7.3 для серверных систем);
  + ЕМИАС 1.0;
  + Операционная система типового дистрибутива АИС ФССП России (GosLinux 6.6);
  + Лотос;
  + РЕД ОС.

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

* возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
* возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
* возможность читать информацию из записей аудита;
* ограничение доступа к чтению записей аудита;
* поиск, сортировка и упорядочение данных аудита;
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
* поддержка определенных ролей их ассоциации с конкретными администраторами безопасности и администраторами серверов или пользователями;
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности;
* возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;
* возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
* возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
* возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов, удаления кода из файлов и системных областей носителей информации;
* возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы;
* отображение сигнала тревоги об обнаружении вредоносного программного обеспечения;
* возможность восстановления функциональных свойств зараженных объектов;
* возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса.

Кроме того, программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

* резидентный антивирусный мониторинг;
* возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени 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;
* настройка возможности управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* возможность добавления точек монтирования в глобальные исключения;
* возможность отслеживать целостность указанных файлов в режиме мониторинга в реальном времени и в режиме проверки по требованию.

1. **Требования к программным средствам антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows**

Средства антивирусной защиты серверов масштаба предприятия и терминальных серверов Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты.

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

* Small Business Server 2008;
* Windows MultiPoint Server 2011№
* Windows Storage Server 2012, 2012 R2, 2016;
* Windows Server 2008, 2008R2;
* Windows Server 2012, 2012 R2;
* Windows Server 2016;
* Windows Hyper-V Server.

Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны функционировать на следующих типах терминальных серверов:

* Microsoft Remote Desktop Services на базе Windows 2008 Server;
* Microsoft Remote Desktop Services на базе Windows 2008 R2 Server;
* Microsoft Remote Desktop Services на базе Windows 2012 Server;
* Microsoft Remote Desktop Services на базе Windows 2012 Server R2;
* Microsoft Remote Desktop Services на базе Windows Server 2016;
* Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15;
* Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15.

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

* возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
* возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
* возможность читать информацию из записей аудита;
* ограничение доступа к чтению записей аудита;
* поиск, сортировка и упорядочение данных аудита;
* возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности;
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
* поддержка определенных ролей их ассоциации с конкретными администраторами безопасности и пользователями;
* возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
* возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
* возможность удаления (если технически возможно) файлов, в которых обнаружен вредоносный код, а также файлов, подозрительных на наличие вредоносного кода, перемещение и изолирование объектов воздействия;
* возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы;
* возможность отображение сигнала тревоги об обнаружении на рабочей станции администратора, в том числе до подтверждения его получения или до завершения сеанса;
* возможность восстановления функциональных свойств зараженных объектов;
* возможность получения и установки обновлений антивирусных баз без применения средств автоматизации, в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения;
* возможность выполнять проверки с целью обнаружения атаки эксплойтов в памяти процессов, в контейнерах Windows Server 2016;
* возможность при обнаружении признаков атаки эксплойтов на защищаемый процесс завершать процесс, сообщать о факте дискредитации уязвимости в процессе.

Кроме того, программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

* антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции (Сервер терминалов и принт-сервер, Сервер приложений и контроллер домена, Файловый сервер);
* 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;
* 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 автоматически запрещение выполнение 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;
* наличие механизмов защиты от эксплуатирования уязвимостей в памяти процессов с помощью техник снижения рисков;
* возможность 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;
* возможность 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);
* возможность интеграции с SIEM системами;
* возможность указания количества рабочих процессов антивируса вручную;
* наличие удаленной и локальной консоли управления;
* возможность 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;

1. **Требования к программным средствам централизованного управления, мониторинга и обновления**

Средства централизованного управления, мониторинга и обновления должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу А не ниже второго класса защиты.

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;
* Microsoft Windows 11;
* Windows Server 2008, 2008R2;
* Windows Server 2012, 2012 R2;
* Windows Server 2016.

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

* Microsoft SQL Server® 2008 Express 32-разрядная;
* Microsoft SQL 2008 R2 Express 64-разрядная;
* Microsoft SQL 2012 Express 64-разрядная;
* Microsoft SQL 2014 Express 64-разрядная;
* Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная;
* Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная;
* Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная;
* Microsoft SQL Server 2012 (все редакции) 64-разрядная;
* Microsoft SQL Server 2014 (все редакции) 64-разрядная;
* Microsoft SQL Server 2016 (все редакции) 64-разрядная;
* Microsoft Azure SQL Database;
* MySQL 5.5 32-разрядная / 64-разрядная (не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5);
* MySQL Enterprise 5.5 32-разрядная / 64-разрядная;
* MySQL 5.6 32-разрядная / 64-разрядная;
* MySQL Enterprise 5.6 32-разрядная / 64-разрядная;
* MySQL 5.7 32-разрядная / 64-разрядная;
* MySQL Enterprise 5.7 32-разрядная / 64-разрядная.

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

* Возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту.
* Возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего.
* Возможность читать информацию из записей аудита.
* Ограничение доступа к чтению записей аудита.
* Поиск, сортировка данных аудита.
* возможность создания учетных записей и аутентификации пользователей;
* возможность администраторам безопасности управлять режимом выполнения функций безопасности
* возможность отображения сигнала тревоги на автоматизированное рабочее место (АРМ) администратора безопасности, указывающего на обнаружение вредоносных компьютерных программ (вирусов) на пользовательских автоматизированных рабочих местах;
* возможность идентифицировать автоматизированные рабочие места, порождающее событие аудита, вредоносные компьютерные программы (вирусы), которые были обнаружены, и действие, предпринятое средством антивирусной защиты;
* возможность продолжать отображение сигнала тревоги на автоматизированном рабочем месте администратора безопасности, пока не будет получено подтверждение его получения или пока не будет завершен сеанс администратора безопасности;
* Возможность получения и установки обновлений антивирусных баз в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения.
* Возможность централизованной установки компонентов антивирусной защиты на серверы и рабочие станции вычислительной сети.
* возможность обработки зараженных объектов на АРМ и серверах вычислительной сети;
* возможность выполнения автоматизированного запуска системы защиты на АРМ и серверах вычислительной сети с заданными условиями поиска и режимами реагирования по расписанию; выполнение удаленного администрирования процессов обнаружения вредоносного программного обеспечения, обновления баз данных и компонентов системы защиты;
* возможность создания учетных записей и аутентификации пользователей.

Кроме того, программные средства централизованного управления, мониторинга и обновления должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

* 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 Active Directory Organization Unit;
* 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 учетной записи, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком Organization Unit находится компьютер или в какой группе безопасности, должна быть реализована возможность поддержки иерархии таких триггеров;
* автоматизированный поиск 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;
* 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 локальным репутационным 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;
* 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 т.д;
* 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 веб-консоли управления приложением;
* наличие системы контроля возникновения вирусных эпидемий.

1. **Требования к обновлению антивирусных баз**

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

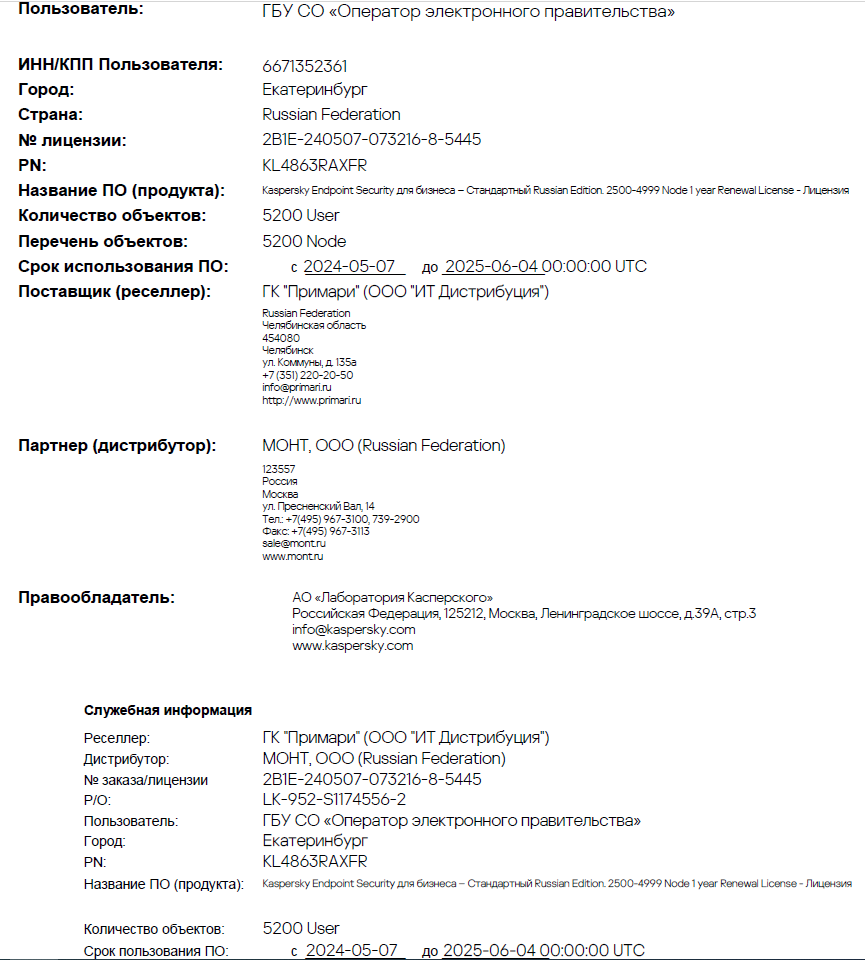
* возможность регламентного обновления антивирусных баз не реже 24 раз в течение календарных суток;
* множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;
* проверка целостности и подлинности обновлений средствами электронной цифровой подписи.

1. **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.



1. Дистрибутив на компакт-диске, содержащий программное обеспечение, права на которые приобретаются в рамках закупки, поставляется в случае, если такое предусмотрено разработчиком (правообладателем) программного обеспечения, или если такая обязанность предусмотрена в нормативно-правовых актах или руководящих документах ФСТЭК. [↑](#footnote-ref-2)