ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Наименование: Оказание услуг по покупке неисключительных (лицензионных) прав использования антивирусного программного обеспечения.

Заказчик заявляет ***продление*** неисключительных (лицензионных) прав антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный 25-49, сроком на 2 года. Действующее количество рабочих мест 26. **Требуемое количество рабочих мест 50** (Лицензирование количества компонентов защиты рабочих станций и файловых серверов должно быть универсальным и ограничиваться только общим количеством защищаемых объектов). Участник размещения заказа не вправе предложить эквивалент, т.к. предложение другого антивирусного программного обеспечения не обеспечит совместимости с существующим у Заказчика программным обеспечением.

Согласно пп. 1 части 1 статьи 33 ФЗ 44 "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" заказчик заявляет о необходимости предоставления в рамках услуги средств защиты информации, совместимых с существующим у Заказчика программным обеспечением Kaspersky Security Center.

№ п/п	Наименование	Единица измерения	Количество
1	Продлении лицензии антивирусной защиты (рабочие станции / файловые сервера)	шт.	50
2	Kaspersky Стандартный Certified Media Pack	шт	1

Номер текущей лицензии Заказчика на право использование программного продукта: 13C8-230627-102916-566-1371**.** *Страна происхождения программного обеспечения – Россия.

Общие требования

Антивирусные средства должны включать:

- программные средства антивирусной защиты для рабочих станций Windows;
- программные средства антивирусной защиты для рабочих станций и серверов Linux;
- программные средства антивирусной защиты для файловых серверов Windows;
- программные средства антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows
- 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

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 должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:

- Windows 7 Home / Professional / Ultimate / Enterprise SP1 (32 / 64-разрядная);
- Windows 8 Professional / Enterprise (32 / 64-разрядная);
- Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
- Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise (TH1, TH2, RS1, RS2,RS3, RS4, RS5, 19H1, 19H2, 20H1, 20H2, 21H1, 21H2) (с ограничениями);
- Windows 11 (21H1) (с ограничениями).

Программные средства антивирусной защиты (далее САВЗ) для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:

- поддержку определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности, администраторами серверов или пользователями;
- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;
- возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;
- получение и установку обновлений в автоматизированном режиме, в том числе с сетевого ресурса;
- получение и установку обновлений без применения средств автоматизации;
- генерацию записи аудита для событий, подвергаемых аудиту;
- чтение информации из записей аудита;
- ассоциацию событий аудита с идентификаторами субъектов;
- ограничение доступа к чтению записей аудита;
- поиск, сортировку, упорядочение данных аудита;
- выполнение проверок 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;
- выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- выполнение проверок с целью обнаружения зараженных объектов по команде;
- выполнение проверок с целью обнаружения зараженных объектов в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
- выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
- удаление (если удаление технически возможно) вредоносного кода из оперативной памяти, удаления файлов, в которых обнаружен вредоносный код, а также файлов, с подозрением на наличие вредоносного кода;
- возможность перемещения и изолирования зараженных объектов, удаления вредоносного кода из файлов и системных областей носителей информации;
- возможность блокирования АРМ, на котором обнаружены зараженные файлы;
- возможность восстановления функциональных свойств зараженных объектов;
- отображение сигнала тревоги об обнаружении вредоносных объектов;
- возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью
- возможность контроля доступа к веб-ресурсам
- возможность контроля за запуском ПО на защищаемом АРМ.

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

- антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;

- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализации действий активного заражения;
- анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
- анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- 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;
- облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
- фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
- проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
- блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
- распознавания и блокировку фишинговых и небезопасных сайтов;
- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
- возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
- контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
- создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или 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, 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;
- 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 управления MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
- записи в журнал событий о записи и/или удалении файлов на съемных дисках;
- контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
- защиты от атак типа BadUSB;
- запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

- защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
- 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 запуска приложения;
- 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 контрольной 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 упрощенной версии графического интерфейса, с минимальным набором возможностей;
- возможность интеграции с Windows Defender Security Center;
- наличие поддержки Antimalware Scan Interface (AMSI);
- наличие поддержки Windows Subsystem for Linux (WSL);
- возможность защитить паролем восстановление объектов из резервного хранилища.
- полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;
- восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, 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 за пределами организации с помощью пароля;
- шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
- возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий).

Требования к программным средствам антивирусной защиты для 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 должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий:

- Windows Small Business Server 2011 Essentials / Standard (64-разрядная);
- Windows MultiPoint Server 2011 (64-разрядная);
- Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная);
- Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная);
- Windows Server 2012 Foundation / Essentials / Standard (64-разрядная);
- Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная);
- Windows Server 2016 (64-разрядная) (с ограничениями);
- Windows Server 2019 (64-разрядная) (с ограничениями)
- Windows Server 2022 (64-разрядная) (с ограничениями).

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

- поддержку определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и администраторами серверов;
- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;
- возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;
- получение и установку обновлений в автоматизированном режиме, в том числе с сетевого ресурса;
- получение и установку обновлений без применения средств автоматизации;
- генерацию записи аудита для событий, подвергаемых аудиту;
- чтение информации из записей аудита;
- ассоциацию событий аудита с идентификаторами субъектов;
- ограничение доступа к чтению записей аудита;
- поиск, сортировку, упорядочение данных аудита;
- выполнение проверок 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;
- выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- выполнение проверок с целью обнаружения зараженных объектов по команде;
- выполнение проверок с целью обнаружения зараженных объектов в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
- выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
- удаление (если удаление технически возможно) вредоносного кода из оперативной памяти, удаления файлов, в которых обнаружен вредоносный код, а также файлов, с подозрением на наличие вредоносного кода;
- возможность перемещения и изолирования зараженных объектов, удаления вредоносного кода из файлов и системных областей носителей информации;
- возможность блокирования АРМ, на котором обнаружены зараженные файлы;
- возможность восстановления функциональных свойств зараженных объектов;
- отображение сигнала тревоги об обнаружении вредоносных объектов;
- возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью
- возможность контроля за запуском ПО на защищаемом 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 из контекстного меню объекта;
- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализации действий активного заражения;
- анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
- анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- 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;
- облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;

- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- 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, 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;
- запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- защиты 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;
- 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 контрольной 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 упрощенной версии графического интерфейса, с минимальным набором возможностей;
- возможность интеграции с Windows Defender Security Center;
- наличие поддержки Antimalware Scan Interface (AMSI);
- наличие поддержки Windows Subsystem for Linux (WSL);
- возможность защитить паролем восстановление объектов из резервного хранилища.

Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux

Средства антивирусной защиты для рабочих станций и 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, В и Г не ниже второго класса защиты.

Программные средства антивирусной защиты для рабочих станций и серверов Linux должны функционировать на компьютерах, работающих под управлением следующих 32-битных операционных систем следующих версий:

- CentOS 6.7, CentOS 6.8, CentOS 6.9, CentOS 6.10;
- Debian GNU/Linux 10.1, Debian GNU/Linux 10.2, Debian GNU/Linux 10.3, Debian GNU/Linux 10.4, Debian GNU/Linux 10.5, Debian GNU/Linux 10.6, Debian GNU/Linux 10.7, Debian GNU/Linux 10.8, Debian GNU/Linux 10.9, Debian GNU/Linux 10.10, Debian GNU/Linux 10.11, Debian GNU/Linux 10.12;
- Debian GNU/Linux 11.0, Debian GNU/Linux 11.1, Debian GNU/Linux 11.2, Debian GNU/Linux 11.3;
- Mageia 4;
- Red Hat Enterprise Linux 6.7, Red Hat Enterprise Linux 6.8, Red Hat Enterprise Linux 6.9, Red Hat Enterprise Linux 6.10;
- Альт 8 СП Рабочая Станция;
- Альт 8 СП Сервер;
- Альт Образование 10;
- Альт Рабочая Станция 10.

Программные средства антивирусной защиты для рабочих станций и серверов Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий:

- AlmaLinux OS 8.5, AlmaLinux OS 8.6;
- AlmaLinux OS 9.0;
- AlterOS 7.5;
- Amazon Linux 2;
- Astra Linux Common Edition 2.12;
- Astra Linux Special Edition (исполнение РУСБ.10015-01) (включая режим замкнутой программной среды и мандатный режим);
- CentOS 6.7, CentOS 6.8, CentOS 6.9, CentOS 6.10;
- CentOS 7.2, CentOS 7.3, CentOS 7.4, CentOS 7.5, CentOS 7.6, CentOS 7.7, CentOS 7.8, CentOS 7.9;
- CentOS Stream 9;
- Debian GNU/Linux 10.1, Debian GNU/Linux 10.2, Debian GNU/Linux 10.3, Debian GNU/Linux 10.4, Debian GNU/Linux 10.5, Debian GNU/Linux 10.6, Debian GNU/Linux 10.7, Debian GNU/Linux 10.8, Debian GNU/Linux 10.9, Debian GNU/Linux 10.10, Debian GNU/Linux 10.11, Debian GNU/Linux 10.12;
- Debian GNU/Linux 11.0, Debian GNU/Linux 11.1, Debian GNU/Linux 11.2, Debian GNU/Linux 11.3;
- EMIAS 1.0;
- EulerOS 2.0 SP5;
- LinuxMint 19.3;
- LinuxMint 20.3;
- openSUSE Leap 15.0, openSUSE Leap 15.1, openSUSE Leap 15.2, openSUSE Leap 15.3, openSUSE Leap 15.4;
- Oracle Linux 7.3, OracleLinux 7.4, OracleLinux 7.5, OracleLinux 7.6, OracleLinux 7.7, OracleLinux 7.8, OracleLinux 7.9;
- Oracle Linux 8.0, Oracle Linux 8.1, Oracle Linux 8.2, Oracle Linux 8.3, Oracle Linux 8.4, Oracle Linux 8.5, Oracle Linux 8.6, Oracle Linux 8.7;
- Red Hat Enterprise Linux 6.7, Red Hat Enterprise Linux 6.8, Red Hat Enterprise Linux 6.9, Red Hat
- Enterprise Linux 6.10;
- Red Hat Enterprise Linux 7.2, Red Hat Enterprise Linux 7.3, Red Hat Enterprise Linux 7.4, Red Hat
- Enterprise Linux 7.5, Red Hat Enterprise Linux 7.6, Red Hat Enterprise Linux 7.7, Red Hat Enterprise Linux 7.8, Red Hat Enterprise Linux 7.9;
- Red Hat Enterprise Linux 8.0, Red Hat Enterprise Linux 8.1, Red Hat Enterprise Linux 8.2, Red Hat
- Enterprise Linux 8.3, Red Hat Enterprise Linux 8.4, Red Hat Enterprise Linux 8.5, Red Hat Enterprise Linux 8.6;
- Red Hat Enterprise Linux 9.0;
- Rocky Linux 8.5, Rocky Linux 8.6;
- SUSE Linux Enterprise Server 12.5;
- SUSE Linux Enterprise Server 15.3;
- Ubuntu 20.04 LTS;
- Ubuntu 22.04 LTS;
- Альт 8 СП Рабочая станция;
- Альт 8 СП Сервер;
- Альт Образование 10;
- Альт Рабочая Станция 10;
- Альт Сервер 10;
- Атлант, сборка Alcyone, версия 2022.02;
- Гослинукс 7.17;
- Гослинукс 7.2;
- РЕД ОС 7.3;
- РОСА "Кобальт" 7.9;
- РОСА "Хром" 12.

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

- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций
- безопасности САВЗ;

- возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций
- безопасности САВЗ;
- получение и установку обновлений в автоматизированном режиме, в том числе с сетевого ресурса;
- получение и установку обновлений без применения средств автоматизации;
- генерацию записи аудита для событий, подвергаемых аудиту;
- чтение информации из записей аудита;
- ассоциацию событий аудита с идентификаторами субъектов;
- ограничение доступа к чтению записей аудита;
- поиск, сортировку, упорядочение данных аудита;
- выполнение проверок 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;
- выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- выполнение проверок с целью обнаружения зараженных объектов по команде;
- выполнение проверок с целью обнаружения зараженных объектов в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
- выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
- удаление (если удаление технически возможно) вредоносного кода из оперативной памяти, удаления файлов, в которых обнаружен вредоносный код, а также файлов, с подозрением на наличие вредоносного кода;
- возможность перемещения и изолирования зараженных объектов, удаления вредоносного кода из файлов и системных областей носителей информации;
- возможность блокирования АРМ и серверов, на которых обнаружены зараженные файлы;
- возможность восстановления функциональных свойств зараженных объектов;
- отображение сигнала тревоги об обнаружении вредоносных объектов.

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

- резидентного антивирусного мониторинга;
- облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- проверку 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;
- антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
- проверку 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);
- защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
- возможность включения опции блокирования файлов во время проверки;
- помещение подозрительных и поврежденных объектов на карантин;
- проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов;
- 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.
- управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;
- проверки съемных дисков;
- отслеживания во входящем сетевом трафике активности, характерной для сетевых атак
- проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым
- получения данных о действиях программ на компьютере пользователя;
- проверки памяти ядра.

Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, 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 файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

32-разрядных операционных систем Microsoft Windows

- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше.

64-разрядных операционных систем Microsoft Windows

- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2008 Standard / Premium;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2011 Essentials / Standard;
- Microsoft Windows MultiPoint™ Server 2011 Standard / Premium;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
- Microsoft Windows MultiPoint Server 2012 Standard / Premium;
- Windows Storage Server 2012;
- Windows Hyper-V Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2016 MultiPoint;
- Windows Server 2016 Core Standard / Datacenter;
- Microsoft Windows MultiPoint Server 2016;
- Windows Storage Server 2016;
- Windows Hyper-V Server 2016;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2019 Core;

- Windows Storage Server 2019;
- Windows Hyper-V Server 2019.
- 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 управлять данными (административными данными), используемыми функциями безопасности;
- возможность уполномоченным пользователям управлять режимом выполнения функций безопасности;
- 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 и Windows Server 2019;
- возможность при обнаружении признаков атаки эксплойтов на защищаемый процесс завершать процесс, сообщать о факте дискредитации уязвимости в процессе;
- возможность проведения проверки целостности компонентов программного изделия.

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: серверов терминалов, 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;
- 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;
- защиты от эксплуатирования уязвимостей в памяти процессов;
- должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
- возможность добавлять процессы в список защищаемых;
- 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;
- возможность указания количества рабочих процессов антивируса вручную;
- 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.
- защита от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
- 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 или локальных пользователей/групп);
- компонент создания специальных правил должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
- компонент создания специальных правил должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, 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;
- наличие механизмов автоматической генерации правил для контроля устройств и приложений.

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 Windows следующих версий:

- Microsoft Windows 11 Home/Pro/Enterprise/Education 64-разрядная
- Windows Server 2008 R2 Standard Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;
- Windows Server 2012 Server Core 64-разрядная; • Windows Server 2012 Datacenter 64-разрядная;
- Windows Server 2012 Essentials 64-разрядная;
- Windows Server 2012 Foundation 64-разрядная;
- Windows Server 2012 Standard 64-разрядная;
- Windows Server 2012 R2 Server Core 64-разрядная;
- Windows Server 2012 R2 Datacenter 64-разрядная;
- Windows Server 2012 R2 Essentials 64-разрядная;
- Windows Server 2012 R2 Foundation 64-разрядная;
- Windows Server 2012 R2 Standard 64-разрядная;
- Windows Server 2016 Datacenter (LTSB) 64-разрядная;
- Windows Server 2016 Standard (LTSB) 64-разрядная;
- Windows Server 2016 (вариант установки Server Core) (LTSB) 64- разрядная;
- Windows Server 2019 Standard 64-разрядная;
- Windows Server 2019 Datacenter 64-разрядная;
- Windows Server 2019 Core 64-разрядная;
- Windows Server 2022 Standard 64-разрядная;
- Windows Server 2022 Datacenter 64-разрядная;
- Windows Server 2022 Core 64-разрядная;
- Windows Storage Server 2012 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Windows Storage Server 2016 64-разрядная;
- Windows Storage Server 2019 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления, под управлением операционных систем Windows, должны функционировать с СУБД следующих версий:

- Microsoft SQL Server 2012 Express 64-разрядная;
- Microsoft SQL Server 2014 Express 64-разрядная;
- Microsoft SQL Server 2016 Express 64-разрядная;
- Microsoft SQL Server 2017 Express 64-разрядная;
- Microsoft SQL Server 2019 Express 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;
- Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная;
- Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная;
- Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная;
- Microsoft Azure SQL Database;
- Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;
- MySQL 5.7 Community 32-разрядная/64-разрядная;
- MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64- разрядная;
- MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 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 10.4.26 и выше) 32-разрядная/64-разрядная;
- MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная;
- MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
- PostgreSQL 13.x 64-разрядная;
- PostgreSQL 14.x 64-разрядная;
- Postgres Pro Standard 13.x 64-разрядная;
- Postgres Pro Standard 14.x 64-разрядная;
- Postgres Pro Certified 14.x 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления, под управлением операционных систем Windows, должны поддерживать установку на следующих виртуальных платформах:

- VMware vSphere 6.7;
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;
- Microsoft Hyper-V Server 2019 64-разрядная;
- Microsoft Hyper-V Server 2022 64-разрядная;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x.
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x (только гостевой вход Windows)

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

- Debian GNU/Linux 11.x (Bullseye) 32-разрядная / 64-разрядная;
- Debian GNU/Linux 10.x (Buster) 32-разрядная / 64-разрядная;
- Debian GNU/Linux 9.x (Stretch) 32-разрядная / 64-разрядная;
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-разрядная / 64- разрядная;
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32-разрядная / 64- разрядная;
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-разрядная / 64- разрядная;
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64-разрядная;
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-разрядная / 64- разрядная;
- CentOS 8.x 64-разрядная;
- CentOS 7.x 64-разрядная;
- CentOS 7.x ARM 64-разрядная;
- Red Hat Enterprise Linux Server 8.x 64-разрядная;
- Red Hat Enterprise Linux Server 7.x 64-разрядная;
- Red Hat Enterprise Linux Server 6.x 32-разрядная / 64- разрядная;
- SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64- разрядная;
- SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64- разрядная;
- SUSE Linux Enterprise Desktop 15 (все пакеты обновлений) 64- разрядная;
- SUSE Linux Enterprise Desktop 15 (пакет обновлений 3) ARM 64-разрядная;
- openSUSE 15 64-разрядная;
- EulerOS 2.0 SP8 ARM;
- Pardus OS 19.1 64-разрядная;
- Astra Linux Special Edition (исполнение РУСБ.10015-01) (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
- Astra Linux Special Edition (исполнение РУСБ.10152-02) (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
- Astra Linux Common Edition 2.12 64-разрядная;
- Альт Сервер 10 64-разрядная;
- Альт Сервер 9.2 64-разрядная;
- Альт Рабочая станция 10 32-разрядная / 64-разрядная;
- Альт Рабочая станция 9.2 32-разрядная / 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 8 СП Рабочая станция (ЛКНВ.11100-01) 32-разрядная /64-разрядная;
- Альт 8 СП Рабочая станция (ЛКНВ.11100-02) 32-разрядная /64-разрядная;
- Альт 8 СП Рабочая станция (ЛКНВ.11100-03) 32-разрядная /64-разрядная;
- Mageia 4 32-разрядная;
- Oracle Linux 7 64-разрядная;
- Oracle Linux 8 64-разрядная;
- Linux Mint 19.x 32-разрядная;
- Linux Mint 20.x 64-разрядная;
- AlterOS 7.5 64-разрядная;

- GosLinux IC6 64-разрядная;
- РЕД ОС 7.3 64-разрядная;
- РЕД ОС 7.3 Сервер 64-разрядная;
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная;
- ROSA Enterprise Linux Server (RELS) 7.3 64-разрядная;
- ROSA Enterprise Linux Desktop (RELD) 7.3 64-разрядная;
- РОСА «КОБАЛЬТ» для клиентских систем 7.3 64-разрядная;
- РОСА «КОБАЛЬТ» для серверов 7.3 64-разрядная;
- Лотос (версия ядра 4.19.50, DE: MATE) 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления, под управлением операционных систем Linux, должны функционировать с СУБД следующих версий:

- MySQL 5.7 Community 32-разрядная / 64-разрядная;
- MySQL 8.0 32-разрядная / 64-разрядная;
- MariaDB 10.5.x 32-разрядная / 64-разрядная;
- MariaDB 10.4.x 32-разрядная / 64-разрядная;
- MariaDB 10.3.22 и выше 32-разрядная / 64-разрядная;
- MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB;
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
- MariaDB 10.1.30 и выше 32-разрядная / 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления, под управлением операционных систем Linux, должны поддерживать установку на следующих виртуальных платформах:

- VMware vSphere 6.7;
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;
- Microsoft Hyper-V Server 2019 64-разрядная;
- Microsoft Hyper-V Server 2022 64-разрядная;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Parallels Desktop 17;
- Виртуальная машина на основе Kernel. Поддерживает следующие операционные системы:
    - Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
    - Альт Сервер 10 64-разрядная;
    - Astra Linux Special Edition (исполнение РУСБ.10015-01) (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
    - Debian GNU/Linux 11.x (Bullseye) 32-разрядная / 64-разрядная;
    - Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
    - РЕД ОС 7.3 Сервер 64-разрядная;
    - РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

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

- генерация записи аудита для событий, подвергаемых аудиту;
- чтение информации из записей аудита;
- ассоциация событий аудита с идентификаторами субъекта;
- ограничение доступа к чтению записей аудита;
- поиск, сортировка данных аудита;
- обработка зараженных объектов на АРМ и серверах вычислительной сети;
- выполнение автоматизированного запуска САВЗ на АРМ и серверах вычислительной сети с заданными условиями поиска вредоносных объектов и режимами реагирования по расписанию;
- выполнение удаленного администрирования процессов обнаружения вредоносных объектов, обновления базы данных признаков вредоносных компьютерных программ (БД ПКВ) и компонентов САВЗ;
- возможность уполномоченным пользователям управлять параметрами настройки функций безопасности САВЗ;
- возможность создания учетных записей и идентификации/аутентификации пользователей;

- отображение сигнала тревоги на автоматизированном рабочем месте администратора безопасности, указывающего на обнаружение вредоносных объектов на пользовательских автоматизированных рабочих местах.
- выполнение получения и установки обновлений БД ПКВ без применения средств автоматизации и в автоматизированном режиме в том числе с сетевого ресурса;
- выполнение централизованной установки компонентов САВЗ.

Кроме того, программные средства централизованного управления, мониторинга и обновления должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК (функционал зависит от операционной системы):

- выбор архитектуры установки централизованного средства управления, мониторинга и обновления 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 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 IPv4-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;
- 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 OU находится компьютер или в какой группе безопасности;
- возможность 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 Exchange ActiveSync (только для Windows);
- функция управления мобильными устройствами через сервер iOS MDM (только для Windows);
- возможность отправки SMS-оповещений о заданных событиях;
- централизованная установка сертификатов на управляемые мобильные устройства (только для Windows);
- 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 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 (только для Windows);
- наличие веб-консоли управления приложением;
- наличие системы контроля возникновения вирусных эпидемий (только для Windows);
- возможность установки в облачной инфраструктуре Microsoft Azure и Google Cloud (только для Windows);
- возможность интеграции по OpenAPI ;
- возможность управления антивирусной защитой с использованием WEB консоли.
- автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей (только для Windows);
- возможность подключения по RDP или штатными средствами из консоли управления, пользователю должен выводиться запрос на разрешение дистанционного подключения (только для Windows);
- наличие инструментов работы с образами ОС: создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры (только для Windows);
- должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;
- возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС (только для Windows);
- возможность импортировать образ операционной системы из дистрибутивов (WIM) (только для Windows);
- наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии (только для Windows);
- автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры (только для Windows);
- поддержка функциональности управления шифрованием данных (только для Windows);
- возможность интеграции с SIEM системами.

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.