**Раздел 3. Техническое задание**

**на оказание услуг по продлению неисключительных прав на использование антивирусного программного обеспечения Kaspersky Endpoint Security для нужд государственного автономного учреждения Саратовской области «Региональный центр оценки качества образования»**

1. **Объем оказываемых услуг включает в себя:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование программного обеспечения | Ед. изм. | Кол-во | Номера действующих лицензий и сроки их окончания**\*** | Срок действия новых лицензий | Конечный пользователь программой |
| 1.1 | Передача неисключительных прав на ПО «Kaspersky Endpoint Security для бизнеса» - Стандартный Russian Edition, 100-149 Node 1 year Renewal License | шт. | 100 | *2922-201221-113552-797-1997*  16.01.2022 г | Не менее чем 12 месяцев | Государственное автономное учреждение Саратовской области «Региональный центр оценки качества образования» |
| 1.2 | Передача Kaspersky Стандартный Certified Media Pack. | шт. | 1 |  | Не менее чем 12 месяцев | Государственное автономное учреждение Саратовской области «Региональный центр оценки качества образования» |

***\* Дата начала новой лицензии приравнивается к дате окончания текущей***

1. **Характеристики Kaspersky Стандартный Certified Media Pack**

Kaspersky Стандартный Certified Media Pack является установочным комплектом комплексного программного средства ПО «Kaspersky Endpoint Security для бизнеса», поставляемого согласно пунктам 1.1, 1.2 настоящего Технического задания, должен содержать:

* Диск с дистрибутивом ПО;
* Формуляр;
* Копию сертификата ФСТЭК и ФСБ России.

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п/п** | **Наименование**  **товара** | **Характеристики товара** | **Кол-во, шт.** |
| **1** | **Программные средства антивирусной защиты** | 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. | **100** |
| 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 / Enterprise (32 / 64-разрядная); * Windows 8 Professional / Enterprise (32 / 64-разрядная); * Windows 8.1 Professional / Enterprise (32 / 64-разрядная); * Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная).   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.   + 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.   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, c 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 (ActiveDirectory 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 ActiveDirectory;   + возможность управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (ActiveDirectory 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 ActiveDirectory;   + 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;   + возможностьинтеграциис Windows Defender Security Center;   + наличиеподдержки Antimalware Scan Interface (AMSI);   + наличиеподдержки Windows Subsystem for Linux (WSL);   + возможность защитить паролем восстановление объектов из резервного хранилища. |
| 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 2008 Standard / Premium (64-разрядная); * 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); * WindowsServer 2016 (64-разрядная) (с ограничениями); * WindowsServer 2019 (64-разрядная) (с ограничениями).   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. * 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 за запуском ПО 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 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; * возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; * создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (ActiveDirectory 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; * возможностьинтеграциис Windows Defender Security Center; * наличиеподдержки Antimalware Scan Interface (AMSI); * наличиеподдержки 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 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 Linux должны функционировать на компьютерах, работающих под управлением следующих 32-битных операционных систем следующих версий:   * Ubuntu 16.04 LTS и выше. * Red Hat Enterprise Linux 6.7 ивыше. * CentOS 6.7 и выше. * Debian GNU / Linux 9.4 и выше. * Debian GNU / Linux 10. * LinuxMint 18.2 и выше. * LinuxMint 19 и выше. * Альт 8 СП Рабочая Станция. * Альт 8 СП Сервер. * Альт Рабочая Станция 8. * Альт Рабочая Станция К 8. * Альт Сервер 8. * Альт Образование 8. * Альт Сервер 9. * Альт Рабочая Станция 9. * Альт Образование 9. * Гослинукс 6.6. * Mageia 4.   Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий:   * Ubuntu 16.04 LTS и выше. * Ubuntu 18.04 LTS и выше. * Red Hat Enterprise Linux 6.7 ивыше. * Red Hat Enterprise Linux 7.2 ивыше. * Red Hat Enterprise Linux 8.0 ивыше. * CentOS 6.7 и выше. * CentOS 7.2 и выше. * CentOS 8.0 и выше. * Debian GNU / Linux 9.4 и выше. * Debian GNU / Linux 10.1 и выше. * OracleLinux 6,7 и выше. * OracleLinux 7,3 и выше. * OracleLinux 8 и выше. * SUSE Linux Enterprise Server 12 SP3 ивыше. * SUSE Linux Enterprise Server 15 ивыше. * openSUSELeap 15 и выше. * Альт 8 СП Рабочая Станция. * Альт 8 СП Сервер. * Альт Рабочая Станция 8. * Альт Рабочая Станция К 8. * Альт Сервер 8. * Альт Образование 8. * Альт Рабочая Станция 9. * Альт Сервер 9. * Альт Образование 9. * AmazonLinux 2. * LinuxMint 18.2 и выше. * LinuxMint 19 и выше. * AstraLinuxSpecialEdition, версия 1.5 (стандартное ядро и ядро PaX). * AstraLinuxSpecialEdition, версия 1.6 (стандартное ядро и ядро PaX). * Astra Linux Common Edition, версия 2.12. * ОС РОСА "КОБАЛЬТ" 7.3 для клиентских систем. * ОС РОСА "КОБАЛЬТ" 7.3 для серверных систем. * Гослинукс 6.6. * Гослинукс 7.2. * AlterOS 7.5 и выше. * Pardus OS 19.1. * RED OS 7.2.   Программные средства антивирусной защиты для рабочих станций и 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; * 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 объекта. * 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:   * 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 (Plaintext); * 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 MicrosoftOutlook 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 MicrosoftWindows   * Windows Server® 2003 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше; * Windows Server 2003 R2 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше; * Windows Server 2008 Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше; * Windows Server 2008 Core / Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше.   64-разрядныхоперационныхсистемMicrosoftWindows   * Windows Server 2003 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше; * Windows Server 2003 R2 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше; * Windows Server 2008 Core Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше; * Windows Server 2008 Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше; * Microsoft Small Business Server 2008 Standard / Premium; * Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше; * Windows Server 2008 Core Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше; * WindowsHyper-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.   ПрограммныесредстваантивируснойзащитыдлясерверовмасштабапредприятияитерминальныхсерверовWindowsдолжныобеспечиватьреализациюследующихфункциональныхвозможностей:   * 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; * 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 WindowsServer 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: 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 MicrosoftWindowsScriptTechnologies (или ActiveScripting), 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 MicrosoftWindows; * 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. |
| 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 10 Enterprise 2016 LTSB 32-разрядная / 64-разрядная; * Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная / 64-разрядная; * Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Pro длярабочихстанций (New in RS3) (Fall Creators Update, v1709) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Pro длярабочихстанций RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Pro длярабочихстанций RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная; * Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная; * Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная; * Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная; * Microsoft Windows 8 Pro 32-разрядная / 64-разрядная; * Microsoft Windows 8 Enterprise 32-разрядная / 64-разрядная; * Microsoft Windows 7 Professional Service Pack 1 32-разрядная / 64-разрядная; * Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-разрядная / 64-разрядная; * Windows Small Business Server 2011 Essentials 64-разрядная; * Windows Small Business Server 2011 Premium Add-on 64-разрядная; * Windows Small Business Server 2011 Standard 64-разрядная; * Windows Small Business Server 2008 Standard / Premium 64-разрядная; * Windows Server 2019 Standard; * Microsoft Windows Server 2019 Datacenter; * Microsoft Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-разрядная; * Microsoft Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-разрядная; * Microsoft Windows Server 2016 (вариантустановки Server Core RS3 (v1709) (LTSB/CBB) 64-разрядная; * Microsoft Windows Server 2016 Standard (LTSB) 64-разрядная; * Microsoft Windows Server 2016 (вариантустановки Server Core) (LTSB) 64-разрядная; * Microsoft Windows Server 2016 Datacenter (LTSB) 64-разрядная; * Microsoft Windows Server 2012 R2 Standard 64-разрядная; * Microsoft Windows Server 2012 R2 Server Core 64-разрядная; * Microsoft Windows Server 2012 R2 Foundation 64-разрядная; * Microsoft Windows Server 2012 R2 Essentials 64-разрядная; * Microsoft Windows Server 2012 R2 Datacenter 64-разрядная; * Microsoft Windows Server 2012 Standard 64-разрядная; * Microsoft Windows Server 2012 Server Core 64-разрядная; * Microsoft Windows Server 2012 Foundation 64-разрядная; * Microsoft Windows Server 2012 Essentials 64-разрядная; * Microsoft Windows Server 2012 Datacenter 64-разрядная; * Windows Server 2008 R2 Standard Service Pack 1 64-разрядная; * Windows Server 2008 with Service Pack 2 (всередакции); * Microsoft Windows Server 2008 Foundation Service Pack 2 32-разрядная / 64-разрядная; * Microsoft Windows Storage Server 2016 64-разрядная; * Microsoft Windows Storage Server 2012 R2 64-разрядная; * Microsoft Windows Storage Server 2012 64-разрядная; * Microsoft Windows Storage Server 2008 R2 64-разрядная.   Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:   * VMware vSphere 6; * VMware vSphere 6.5; * VMware Workstation 14 Pro; * Microsoft Hyper-V Server 2008 64-разрядная; * Microsoft Hyper-V Server 2008 R2 64-разрядная; * Microsoft Hyper-V Server 2008 R2 Service Pack 1 64-разрядная; * Microsoft Hyper-V Server 2012 64-разрядная; * Microsoft Hyper-V Server 2012 R2 64-разрядная; * Microsoft Hyper-V Server 2016 64-разрядная; * Citrix XenServer 7; * Citrix XenServer 7.1 LTSR; * ParallelsDesktop 11; * Oracle VM VirtualBox 5.x.   Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:   * Microsoft SQL Server 2008 Express 32-разрядная; * Microsoft SQL Server 2008 R2 Express 64-разрядная; * 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 2008 (все редакции) 32-разрядная / 64-разрядная; * Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная; * Microsoft SQL Server 2008 R2 Service Pack 2 (всередакции) 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 SQL Server 2017 (все редакции) для Windows 64-разрядная; * MySQL Standard Edition 5.6 32-разрядная / 64-разрядная; * MySQL Enterprise Edition 5.6 32-разрядная / 64-разрядная; * MySQL Standard Edition 5.7 32-разрядная / 64-разрядная; * MySQL Enterprise Edition 5.7 32-разрядная / 64-разрядная; * Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и MicrosoftAzure;   В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:   * 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 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, генерирующие события аудита, вредоносные компьютерные программы (вирусы), которые были обнаружены, и действия, предпринятые средствами 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 объекта, обновления баз данных и компонентов системы защиты; * возможность создания внутренних учетных записей для аутентификации пользователей.   Кроме того, программные средства централизованного управления, мониторинга и обновления должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:   * выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов; * возможность чтения информации из ActiveDirectory, 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 ExchangeActiveSync; * функция управления мобильными устройствами через сервер iOS MDM; * возможность отправки SMS-оповещений о заданных событиях; * централизованная установка сертификатов на управляемые мобильные устройства; * 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; * автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на компьютерах с ОС Windows * 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; * поддержкаинтеграциис Windows сервисом Certificate Authority; * наличие веб-консоли управления приложением; * наличие портала самообслуживания пользователей; * портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя; * наличие системы контроля возникновения вирусных эпидемий; * возможность установки в облачной инфраструктуре MicrosoftAzure и GoogleCloud; * возможность интеграции по OpenAPI; * возможность управления антивирусной защитой с использованием WEB консоли. |
| 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. |

1. **Условия передачи неисключительных прав на ПО**
   1. Исполнитель должен предоставить:

* ключи активации (продления) на основании оригинала лицензионного соглашения с компанией правообладателем данного программного обеспечения на бумажном носителе;
* медиа-паки, включающие в себя диски с записанными сертифицированными приложениями и формуляры, промаркированные уникальным идентификатором системы сертификации № РОСС RU.01;
  1. ***Поставка эквивалента невозможна в связи с необходимостью обеспечения совместимости с существующей инфраструктурой. Система антивирусной защиты на основе программ Антивируса Касперского уже внедрена у Заказчика. Поставляемый Товар не должен приводить к нарушению работоспособности имеющихся сервисов или ухудшению эксплуатационных характеристик программного и аппаратного обеспечения компьютеров, эксплуатируемых заказчиком, к накладным расходам по замене программного обеспечения.***