|  |  |
| --- | --- |
|  | Приложение №1 котировочной документацииУтверждаюГлавный врачЧУЗ «РЖД-Медицина» г. Калининград»\_\_\_\_\_\_\_\_\_\_\_\_\_Л.М. Сиглаева м.п. |

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на оказание услуг по продлению Kaspersky Endpoint Security для бизнеса – Стандартный для ЧУЗ "РЖД-МЕДИЦИНА" Г. КАЛИНИНГРАД"**

1. **Наименование и описание объекта закупки (функциональные, технические и качественные характеристики, эксплуатационные характеристики объекта закупки), объем и условия оказания услуг, требования к качеству услуг:**

 **1.1. Наименование объекта закупки:** оказание услуг по продлению лицензии Kaspersky Endpoint Security для бизнеса – Стандартный

 **1.2. Описание услуг, объем и условия оказания услуг, требования к качеству услуг:**

|  |  |
| --- | --- |
| **Наименование**  | Продление лицензии пользователя (передача неисключительных прав на использование программ для ЭВМ) ЧУЗ "РЖД-МЕДИЦИНА" Г. КАЛИНИНГРАД"№26FE-180910-144526-7-1559, лицензия на 2 года, программное обеспечение Kaspersky Endpoint Security для бизнеса – Стандартный 50-99 NodeRenewal 2 yearKL4863RAQDR \* |
| **Количество закупаемых товаров, объем работ, услуг** | Лицензия на 70 рабочих места |
| **Место поставки** | 236005, КАЛИНИНГРАДСКАЯ ОБЛ, КАЛИНИНГРАД Г, ЛЕТНЯЯ УЛ, 1 |
| **Срок (периодичность) передачи неисключительных лицензионных прав** | Поставщик передает неисключительные лицензионные права Заказчику в срок не позднее 30 (тридцати) календарных дней в полном объеме с момента заключения государственного контракта. |
| **Условия поставки товара** | Датой передачи неисключительных лицензионных прав, считается дата подписания Акта приема передачи неисключительных прав, **без претензий**. |
| **Требования по объему и сроку гарантий качества товаров** | Поставщик гарантирует работу ключа на программный продукт в течение 24 месяцев при соблюдении условий лицензионного соглашения. Гарантийные обязательства вступают в силу с момента приема передачи неисключительных прав заказчику. |

\* данное программное обеспечение (далее ПО) не сопровождается словами «или эквивалент», так как необходимо обеспечить взаимодействие указанного ПО с базами данных и другим ПО, которые используются Заказчиком.

**1.3. Технические требования к системе антивирусной защиты: KasperskyEndpointSecurity для бизнеса – Стандартный**

# **Общие требования**

Антивирусные средства должны включать:

* программные средства антивирусной защиты для рабочих станций Windows;
* программные средства антивирусной защиты для рабочих станций MacOS;
* программные средства антивирусной защиты для рабочих станций Linux;
* программные средства антивирусной защиты для файловых серверов Windows;
* программные средства антивирусной защиты для файловых серверов Linux;
* программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов);
* программные средства централизованного управления, мониторинга и обновления;
* обновляемые базы данных сигнатур вредоносных программ и атак;
* эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.

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

# **Требования к программным средствам антивирусной защиты для рабочих станций Windows**

Программные средства антивирусной защиты 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).

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

* 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 прощенной 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**

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).

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

* 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 прощенной 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 Mac**

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

* macOS Catalina 10.15;
* macOSMojave 10.14;
* macOSHighSierra 10.13;
* macOSSierra 10.12.

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

* резидентный антивирусный мониторинг;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* автоматическое обновление антивирусных баз по расписанию;
* резервное копирование зараженных файлов перед их удалением, для возможности восстановления;
* эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
* защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* проверку сетевого трафика, передаваемого через браузеры Safari, GoogleChrome и Firefox (HTTP и HTTPS трафик);
* контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

# **Требования к программным средствам антивирусной защиты для рабочих станций Linux**

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

* Ubuntu 16.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 и выше;
* Debian GNU / Linux 8.6- 8.х;
* Debian GNU / Linux 9.4 – 9.х;
* LinuxMint 18.2 – 18.х;
* LinuxMint 19 (последняя версия);
* Альт Линукс СПТ 7.0.6;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* Лотос;
* Гослинукс 6.6.

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

* Ubuntu 16.04 LTS;
* Ubuntu 18.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 – 6.х;
* CentOS 7.2 – 7.х;
* Debian GNU / Linux 8.6- 8.х;
* Debian GNU / Linux 9.4 – 9.х;
* OracleLinux 7.3 и выше;
* SUSE LinuxEnterpriseServer 15;
* openSUSE 15;
* Альт Линукс СПТ 7.0.6 ;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* AmazonLinux AMI;
* LinuxMint 18.2 и выше;
* LinuxMint 19 (последняя версия);
* Micro Focus Open Enterprise Server 2018;
* AstraLinuxSpecialEdition 1.5 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* AstraLinuxSpecialEdition 1.6 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* Циркон 36КТ;
* Циркон 36СТ;
* ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем;
* ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем;
* ЕМИАС 1.0;
* Гослинукс 6.6;
* Лотос;
* РЕД ОС 7.2.

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

* 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;
* 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.

**Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows**

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® 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-разрядныхоперационныхсистем Microsoft Windows**

* Windows Server 2003 Standard / Enterprise / Datacenter с пакетомобновлений SP2 иливыше;
* Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетомобновлений SP2 иливыше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* Windows Server 2008 Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* Microsoft Small Business Server 2008 Standard / Premium;
* Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* WindowsHyper-VServer 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.

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

* 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 WindowsScriptTechnologies (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 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.

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

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;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 и выше;
* Debian GNU / Linux 8.6 – 8.х;
* Debian GNU / Linux 9.4 - 9.х;
* LinuxMint 18.2 и выше;
* LinuxMint 19 (последняя версия);
* Альт Линукс СПТ 7.0.6;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* Лотос;
* Гослинукс 6.6.

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

* Ubuntu 16.04 LTS;
* Ubuntu 18.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 – 6.х;
* CentOS 7.2 – 7.х;
* Debian GNU / Linux 8.6 – 8.х;
* Debian GNU / Linux 9.4 - 9.х;
* OracleLinux 7.3 и выше;
* SUSE LinuxEnterpriseServer 15;
* openSUSE 15;
* Альт Линукс СПТ 7.0.6;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* AmazonLinux AMI;
* LinuxMint 18.2 и выше;
* LinuxMint 19 (последняя версия);
* Micro Focus Open Enterprise Server 2018;
* AstraLinuxSpecialEdition 1.5 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* AstraLinuxSpecialEdition 1.6 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* Циркон 36КТ;
* Циркон 36СТ;
* ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем;
* ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем;
* ЕМИАС 1.0;
* Гослинукс 6.6;
* Лотос;
* РЕД ОС 7.2.

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

* 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;
* помещение подозрительных и поврежденных объектов на карантин;
* проверку почтовых баз приложений Microsoft Outlook
* возможность перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию;
* возможность управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

# Требования к программным средствам антивирусной защиты мобильных устройств

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

* Android 4.4– 10.0;
* AppleiOS 10.0 – 12.

В программном средстве антивирусной защиты смартфонов для ОС Android должны быть реализованы следующие функциональные возможности:

* постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;
* проверка файловой системы устройства по требованию и по расписанию;
* мгновенная проверка устанавливаемых приложений
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* поддержка белых списков разрешенных сайтов;
* наличие хранилища для изолирования зараженных объектов;
* обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;
* блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;
* поддержка белых списков разрешенных приложений;
* блокировка системных приложений, в рамках контроля запуска приложений;
* возможность отправки команд и push уведомлений через сервис FirebaseCloudMessaging (FCM);
* базовая поддержка AndroidforWork;
* возможность заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
* возможность указать параметры подключения к wi-fi сетям;
* возможность указать обязательные к установке приложения;
* возможность блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factoryreset);
* возможность создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
* поддержка технологий Samsung KNOX1 и KNOX2.

В программном средстве защиты смартфонов для ОС AppleiOS должны быть реализованы следующие функциональные возможности:

* возможность удаленной настройки параметров iOSMDM-устройств с помощью групповых политик;
* возможность отправки команды блокирования и удаления данных;
* возможность создавать групповые политики безопасности мобильных устройств;
* удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу ExchangeActiveSync\ iOSMDM;
* получать отчеты и статистику о работе мобильных устройств пользователей;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervisedmode;
* возможность централизованного управления с помощью единой консоли управления.

# **Требования к программным средствам централизованного управления, мониторинга и обновления**

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

* Microsoft Windows 7 32-разрядная / 64-разрядная;
* Microsoft Windows 8 32 разрядная / 64-разрядная;
* Microsoft Windows 8;1 32-разрядная / 64-разрядная;
* Microsoft Windows 10 32-разрядная / 64-разрядная;
* Windows Server 2008, 2008 R232-разрядная / 64-разрядная;
* Windows Server 2012, 2012 R264-разрядная;
* Windows Server 2016 64-разрядная;
* WindowsServer 2019 Standard, Datacenter.

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

* VMware vSphere 5.5, 6;
* VMware Workstation 12.x Pro;
* Microsoft Hyper-V Server 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2;
* Microsoft Virtual PC 2007 (6.0.156.0);
* Citrix XenServer 6.2, 6.5, 7;
* Parallels Desktop 11 для Mac;
* OracleVMVirtualBox 4.0.4-70112 (поддерживаются гостевые операционные системы Windows).

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

* Microsoft SQL Server 2008 Express 32-разрядная;
* Microsoft SQL 2008 R2 Express 64-разрядная;
* Microsoft SQL 2012 Express, 2014 Express 64-разрядная;
* MicrosoftSQLServer 2008 (все редакции) 32-разрядная / 64-разрядная;
* MicrosoftSQLServer 2008 R2 (все редакции) 64-разрядная;
* Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная;
* MicrosoftSQLServer 2012 (все редакции) 64-разрядная;
* MicrosoftSQLServer 2014 (все редакции) 64-разрядная;
* MicrosoftSQLServer 2016 (все редакции) 64-разрядная;
* Microsoft SQL Server 2017 (для Windows) 64-разрядная;
* Microsoft Azure SQL Database;
* MySQL 5.5 32-разрядная / 64-разрядная (не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5);
* MySQL Enterprise 5.5 32-разрядная / 64-разрядная;
* MySQL 5.6 32-разрядная / 64-разрядная;
* MySQL Enterprise 5.6 32-разрядная / 64-разрядная;
* MySQL 5.7 32-разрядная / 64-разрядная;
* MySQLEnterprise 5.7 32-разрядная / 64-разрядная.

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

* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* 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 OUAD;
* автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OUAD;
* 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 iOSMDM;
* 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;
* 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;
* поддержкаинтеграции с Windows сервисом Certificate Authority;
* наличие веб-консоли управления приложением;
* наличие портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* возможность установки в облачной инфраструктуре Microsoft Azure;
* 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 телефону, 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.

Техническое задание согласовано \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Шидловский С. А.