Утверждаю

Директор по безопасности –

начальник отдела безопасности

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Брянкин А.Б.

«\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2021 г

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

Антивирусное программное обеспечение должно предоставлять АО «НИИМЭ» (Заказчику) защиту информации корпоративной сети на **12 месяцев на 700 защищаемых объектов**. Лицензирование количества компонентов защиты рабочих станций и файловых серверов должно быть универсальным и ограничиваться только общим количеством защищаемых объектов в течение срока действия лицензионного соглашения. **Антивирусное программное обеспечение должно производить шифрование данных и включать модуль расширенного системного администрирования, а также быть совместимым с существующим у Заказчика программным обеспечением Kaspersky Security Center.**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование объекта закупки | Единица измерения | Количество |
| 1. | Программное средство антивирусной защиты | шт. | 1 |

Услуги по передаче неисключительного права на использование антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition 5000+ Node 1 year Renewal License: Kaspersky Security for WS and FS на 12 месяцев на 700 защищаемых объектов для нужд АО «НИИМЭ».

Передача права на эквивалентные программные продукты не допустима, так как иные программные средства не обеспечат совместимости с уже эксплуатируемым Заказчиком программным обеспечением и уже имеющимися правами на использование программного обеспечения, что повлечет дополнительные расходы Заказчика по интеграции программного обеспечения и обучению персонала.

Заказчик имеет действующие соглашения:

* № 17E0-200210-124825-203-448 от правообладателя АО «Лаборатория Касперского» на 150 защищаемых объектов (рабочие станции / файловые сервера / мобильные устройства). Срок окончания действия лицензионного ключа – 30.04.2021;
* № 17E0-180621-125653-263-1442 от правообладателя АО «Лаборатория Касперского» на 350 защищаемых объектов (рабочие станции / файловые сервера / мобильные устройства). Срок окончания действия лицензионного ключа – 30.04.2021.

Срок действия лицензии 12 месяцев, срок начала действия лицензии «30» апреля 2021 г., окончания действия лицензии «30» апреля 2024 года. Срок поставки лицензии до «30» апреля.2021 г.

Поставка программного средства антивирусной защиты должна осуществляться Поставщиком в рамках действующего Партнерского соглашения с АО «Лаборатория Касперского».С целью принятия исчерпывающих мер по обеспечению антивирусной защиты информации к программному обеспечению, Исполнителю необходимо предоставить Заказчику право на:

* использование новых версий антивирусного программного обеспечения или отдельных его модулей по мере их выхода (через сеть интернет);
* использование услуг технической поддержки (по телефону и/или через сеть интернет);
* доступ к информационным и вспомогательным ресурсам правообладателя программного обеспечения, в том числе к антивирусным базам данных, содержащие описания сигнатур угроз и сетевых атак, а также методы борьбы с ними.

**Общие требования**

Антивирусные средства должны включать:

* Программные средства антивирусной защиты для рабочих станций Windows;
* Программные средства антивирусной защиты для файловых серверов Windows;
* Программные средства антивирусной защиты для рабочих станций MacOS;
* Программные средства антивирусной защиты для рабочих станций Linux;
* 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;
* Программные средства обнаружения, оценки и закрытия уязвимостей в установленных приложениях;
* Программные средства инвентаризации установленного программного обеспечения и оборудования;
* Программные средства шифрования данных;
* Обновляемые базы данных сигнатур вредоносных программ и атак;
* Техническую поддержку;
* Универсальную лицензию антивирусной защиты для рабочих станций, файловых серверов, мобильных устройств c возможностью изменения соотношения защищаемых объектов в течение срока действия лицензионного соглашения в рамках приобретаемого числа лицензий.

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 / Ultimate / Enterprise Service Pack 1 и выше (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 (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* возможность управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
* записи в журнал событий о записи и/или удалении файлов на съемных дисках;
* контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
* защиты от атак типа BadUSB;
* запуск специальной задачи для обнаружения закрытия 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;
* установка 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 файла, 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;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* возможность защитить паролем восстановление объектов из резервного хранилища.
* полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии SingleSignOn, поддержка UEFI-систем;
* восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем;
* поддержка двухфакторной аутентификации при полнодисковом шифровании;
* шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению);
* наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля;
* шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
* возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий).

**Требования к программным средствам антивирусной защиты для серверов Windows**

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);
* Windows Server 2016 (64-разрядная) (с ограничениями);
* Windows Server 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 (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
	+ запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
	+ защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
	+ установка 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;
	+ наличие поддержки Antimalware Scan Interface (AMSI);
	+ наличие поддержки Windows Subsystem for Linux (WSL);
	+ возможность защитить паролем восстановление объектов из резервного хранилища.
	+ возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий).

**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 10.15;
* macOS 10.14;
* macOS 10.13;
* macOS 11.0.

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, Google Chrome 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 с возможностью управлять шифрованием FileVault.

**Требования к программным средствам антивирусной защиты для рабочих станций и 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 и выше;
* Red Hat® Enterprise Linux® 6.7 выше;
* CentOS 6.7 и выше;
* Debian GNU / Linux 9.4 и выше;
* Debian GNU / Linux 10;
* Linux Mint 18.2 ивыше;
* LinuxMint 19 и выше;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.3 Рабочая станция;
* Альт Линукс 8.3 Рабочая станция К;
* Альт Линукс 8.3 Сервер;
* Альт Линукс 8.3 Образование;
* Альт Линукс 9 Рабочая станция;
* Альт Линукс 9 Образование;
* Гослинукс 6.6;
* Mageia 4.

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 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 7.3 и выше;
* OracleLinux 8 ивыше;
* SUSE® Linux Enterprise Server 15 ивыше;
* openSUSE® Leap 15 ивыше;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.3 Рабочая станция;
* Альт Линукс 8.3 Рабочая станция К;
* Альт Линукс 8.3 Сервер;
* Альт Линукс 8.3 Образование;
* Альт Линукс 9 Рабочая станция;
* Альт Линукс 9 Сервер;
* Альт Линукс 9 Образование;
* Amazon Linux AMI;
* Linux Mint 18.2 ивыше;
* LinuxMint 19 и выше;
* AstraLinuxSpecialEdition 1.5 (обычный режим и режим замкнутой программной среды);
* AstraLinuxSpecialEdition 1.6 (обычный режим и режим замкнутой программной среды);
* Astra Linux Common Edition «Орел» 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.

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;
	+ возможность проверки памяти ядра;
	+ 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 или веб-консоли;
	+ возможность управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;
	+ возможность проверки съемных дисков;
	+ возможность отслеживания во входящем сетевом трафике активности, характерной для сетевых атак;
	+ возможность проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым веб-адресам.

**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 10 Enterprise 2019 LTSC 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Pro для рабочих станций 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 10 Pro 19H1 32-разрядная / 64-разрядная;
* MicrosoftWindows 10 Pro для рабочих станций 19H1 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Enterprise 19H1 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Education 19H1 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Pro 19H2 32-разрядная / 64-разрядная;
* MicrosoftWindows 10 Pro для рабочих станций 19H2 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Enterprise 19H2 32-разрядная / 64-разрядная;
* Microsoft Windows 10 Education 19H2 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;
* Microsoft Windows Server 2019 Standard 64-разрядная;
* Microsoft Windows Server 2019 Datacenter 64-разрядная;
* 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 (вариант установки Server Core RS3 (v1709) (LTSB/CBB) 64-разрядная;
* Microsoft Windows Server 2016 Standard (LTSB) 64-разрядная;
* Microsoft Windows Server 2016 (вариант установки 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;
* Microsoft Windows Storage Server 2016 64-разрядная;
* Microsoft Windows Storage Server 2012 R2 64-разрядная;
* Microsoft Windows Storage Server 2012 64-разрядная.

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

* VMware vSphere 6.5;
* VMware vSphere 6.7;
* VMware Workstation 15 Pro;
* Microsoft Hyper-V Server 2012 64-разрядная;
* Microsoft Hyper-V Server 2012 R2 64-разрядная;
* Microsoft Hyper-V Server 2016 64-разрядная;
* Microsoft Hyper-V Server 2019 64-разрядная;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 14;
* Oracle VM VirtualBox 6.x.

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

* Microsoft SQL Server 2012 Express 64-разрядная;
* Microsoft SQL Server 2014 Express 64-разрядная;
* Microsoft SQL Server 2016 Express 64-разрядная;
* Microsoft SQL Server 2017 Express 64-разрядная;
* Microsoft SQL Server 2019 Express 64-разрядная;
* Microsoft SQL Server 2014 (все редакции) 64-разрядная;
* Microsoft SQL Server 2016 (все редакции) 64-разрядная;
* Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;
* Microsof tSQL Server 2017 (все редакции) для Linux 64-разрядная;
* Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная;
* Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная;
* 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 Microsoft Azure;
* MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB.

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 Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
	+ возможность настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
	+ автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;
	+ централизованные установка, обновление и удаление программных средств антивирусной защиты;
	+ централизованная настройка, администрирование;
	+ просмотр отчетов и статистической информации по работе средств защиты;
	+ централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
	+ сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
	+ наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
	+ возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
	+ возможность иерархии триггеров, по которым происходит перераспределение;
	+ тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
	+ доставка обновлений на рабочие места пользователей сразу после их получения;
	+ распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
	+ построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
	+ создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
	+ поддержка мультиарендности (multi-tenancy) для серверов управления;
	+ обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
	+ доступ к облачным серверам производителя антивирусного ПО через сервер управления;
	+ автоматическое распространение лицензии на клиентские компьютеры;
	+ инвентаризация установленного ПО и оборудования на компьютерах пользователей;
	+ наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
	+ функция управления мобильными устройствами через сервер Exchange ActiveSync;
	+ 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;
	+ построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
	+ наличие преднастроенных стандартных отчетов о работе системы;
	+ экспорт отчетов в файлы форматов PDF и XML;
	+ централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
	+ создание внутренних учетных записей для аутентификации на сервере управления;
	+ создание резервной копии системы управления встроенными средствами системы управления;
	+ поддержка Windows Failover Clustering;
	+ поддержка интеграции с Windows сервисом Certificate Authority;
	+ наличие веб-консоли управления приложением;
	+ наличие портала самообслуживания пользователей;
	+ наличие системы контроля возникновения вирусных эпидемий;
	+ возможность установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
	+ возможность интеграции по OpenAPI;
	+ возможность управления антивирусной защитой с использованием WEB консоли;
	+ автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
	+ наличие преднастроенных ролей пользователей средств централизованного управления;
	+ возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей;
	+ возможность подключения по RDP или штатными средствами из консоли управления;
	+ пользователю должен выводиться запрос на разрешение дистанционного подключения;
	+ наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на «голое железо» (baremetal);
	+ должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;
	+ возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС;
	+ возможность импортировать образ операционной системы из дистрибутивов (WIM);
	+ наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии;
	+ автоматическое создание установочных пакетов для сторонних приложений (AdobeReader, MozillaFirefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры;
	+ поддержка функциональности управления шифрованием данных;
	+ возможность интеграции с SIEM системами, и передача событий в формате syslog или CEF\ LEEF.

**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 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.

**Требования к поставке антивирусного программного обеспечения и сертификатов соответствия**

Исполнитель подтверждает передачу неисключительных прав на использование антивирусного программного обеспечения путём предоставления электронных лицензионных ключей активации на физическом носителе официального исполнения.

Руководитель проектов по ИБ Григорьев Г.Н.

Согласовано:

Начальник ОИТ Капичников Д.В.