ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ «НАВОИЙУРАН»

УТВЕРЖДАЮ
Директор по ИТ и цифровизации
ГП « Навоийуран »
_____ И.К. Халиков
«___» 05 2022 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на закупку программного обеспечения
для антивирусной защиты серверов и компьютеров

На 28 листах

СОДЕРЖАНИЕ:

Раздел 1. Наименование и цели использования выполненных работ и оказываемых услуг с указанием основных технико-экономических показателей.

Наименование услуги - Программное обеспечение для антивирусной защиты серверов и компьютеров.

Основной целью программного обеспечения:

- обеспечение антивирусной защищенности информационно-коммуникационных систем от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок;
- предотвращение внедрения вредоносных программ в информационных системы;
- выявление и безопасное удаление из систем в случае попадания;
- фильтрация доступа пользователей предприятия к непродуктивным интернет ресурсам.

Раздел 2. Основание для реализации проекта, в рамках которого производится закупка.

Основаниями для реализации проекта, в рамках которого производится закупка:

- Постановление Президента Республики Узбекистан от 15.12.2010г. №ПП-1442 «О мерах развития промышленности Республики Узбекистан в 2011-2015гг»;
- Указ Президента Республики Узбекистан от 04.03.2015г. №УП-4707 «О программе мер по обеспечению структурных преобразований, модернизации и диверсификации производства в 2015-2019годах»;
- Постановление Президента Республики Узбекистан от 03.04.2014г. №ПП-2158 «О мерах по дальнейшему внедрению информационно-коммуникационных технологий в реальном секторе экономики»
- Постановление Кабинета Министров №295 от «16» октября 2015 г. «Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан»
- O`z DSt ISO/IEC 27011:2014 Информационная технология. Методы обеспечения безопасности. Руководящие указания по управлению информационной безопасностью в организациях телекоммуникаций.
- O`z DSt ISO/IEC 15408-1, 2, 3:2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
- O`z DSt ISO/IEC 13335-1:2009 Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационно-коммуникационных технологий. (Часть 1). Концепции и модели управления безопасностью информационнокоммуникационных технологий.
- O`z DSt ISO/IEC TR 15446:2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.
- O`z DSt ISO/IEC 27001-2009 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.
- O`z DSt ISO/IEC 27002-2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.
- O`z DSt 2814:2014 Информационная технология. Автоматизированные системы. Классификация по уровню защищённости от несанкционированного доступа к информации.

- O`z DSt 2817:2014 Информационная технология. Средства вычислительной техники. Классификация по уровню защищённости от несанкционированного доступа к информации.
- RH 45-170:2004 «Основные технические требования по созданию локальных и корпоративных ведомственных компьютерных сетей»
- T 45-194:2007 «Рекомендации по применению программно-аппаратных средств, обеспечивающих предотвращение актов незаконного проникновения в информационные системы».

Раздел 3. Перечень работ, услуг и их объёмы (количество) требуемые от исполнителя с учётом реальных потребностей и их обоснованием исходя из требований действующих нормативных актов.

Основной перечень работ для Исполнителя (компания-поставщик, выигравшая закупочные процедуры на поставку программного обеспечения, далее – Исполнитель):

1. Поставка программного обеспечения.
2. Техническая поддержка в течение 2 лет.

Поставляется клиентская лицензия программного обеспечения в количестве 1000 шт.

При этом, для расширения круга потенциальных участников в закупочных процедурах, Заказчиком будут рассматриваться аналогичное по функциональности либо не уступающее характеристиками программное обеспечение, указанное в Техническом задании.

Общие требования

Антивирусные средства должны включать:

- программные средства антивирусной защиты для рабочих станций Windows;
- программные средства антивирусной защиты для 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, серверов масштаба предприятия, терминальных серверов Windows;
- программные средства антивирусной защиты для файловых серверов Linux;
- программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов);
- программные средства антивирусной защиты виртуальных сред с использованием агентов;
- 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:

- антивирусного сканирования в режиме реального времени и по запросу из контекстного меню объекта;
- антивирусного сканирования 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 следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
- фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
- проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
- блокировку баннеров и всплывающих окон на загружаемых Web-страницах;

- распознавания и блокировку фишинговых и небезопасных сайтов;
- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защиту от сетевых угроз 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;
- 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 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;
- контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
- возможность управления MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
- записи в журнал событий о записи и/или удалении файлов на съемных дисках;
- контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
- защиты от атак типа BadUSB;
- запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;
- восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем;
- поддержка двухфакторной аутентификации при полнодисковом шифровании;
- шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению);
- наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля;
- шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
- 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 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;
- возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);
- возможность интеграции с Windows Defender Security Center;
- наличие поддержки Antimalware Scan Interface (AMSI);
- наличие поддержки Windows Subsystem for Linux (WSL);
- возможность защитить паролем восстановление объектов из резервного хранилища.

Требования к программным средствам антивирусной защиты для 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;
- установки только выбранных компонентов программного средства антивирусной защиты;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- возможность проверки целостности антивирусной программы;
- возможность добавления исключений из антивирусной проверки по хеш сумме файл, маске

имени/директории или по наличию у файла доверенной цифровой подписи;
- наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
- наличие защищенного хранилища для отчетов о работе антивируса;
- возможность включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
- возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);
- возможность интеграции с Windows Defender Security Center;
- наличие поддержки Antimalware Scan Interface (AMSI);
- наличие поддержки Windows Subsystem for Linux (WSL);
- возможность защитить паролем восстановление объектов из резервного хранилища.

Требования к программным средствам антивирусной защиты для рабочих станций Mac

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

- macOS Catalina 10.15;
- macOS Mojave 10.14;
- macOS High Sierra 10.13;
- macOS Sierra 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, 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 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.x;
– Red Hat Enterprise Linux 7.2 – 7.x;
– CentOS 6.7 и выше;
– Debian GNU / Linux 8.6- 8.x;
– Debian GNU / Linux 9.4 – 9.x;
– Linux Mint 18.2 – 18.x;
– Linux Mint 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.x;
– Red Hat Enterprise Linux 7.2 – 7.x;
– CentOS 6.7 – 6.x;
– CentOS 7.2 – 7.x;
– Debian GNU / Linux 8.6- 8.x;
– Debian GNU / Linux 9.4 – 9.x;
– OracleLinux 7.3 и выше;
– SUSE Linux Enterprise Server 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;
- Amazon Linux AMI;
- Linux Mint 18.2 и выше;
- Linux Mint 19 (последняя версия);
- Micro Focus Open Enterprise Server 2018;
- Astra Linux Special Edition 1.5 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
- Astra Linux Special Edition 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.

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

- резидентного антивирусного мониторинга;
- облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- проверку ресурсов доступных по SMB / NFS;
- эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;
- проверку сообщений электронной почты в текстовом формате (Plain text);
- наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
- защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
- 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 с пакетом обновлений SP2 или выше;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше.

64-разрядных операционных систем Microsoft Windows:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2008 Standard / Premium;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;
- Microsoft Small Business Server 2011 Essentials / Standard;
- Microsoft Windows MultiPoint™ Server 2011 Standard / Premium;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
- Microsoft Windows MultiPoint Server 2012 Standard / Premium;
- Windows Storage Server 2012;
- Windows Hyper-V Server 2012;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
- Windows Storage Server 2012 R2;
- Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials / Standard / Datacenter;

- Windows Server 2016 MultiPoint;
- Windows Server 2016 Core Standard / Datacenter;
- Microsoft Windows MultiPoint Server 2016;
- Windows Storage Server 2016;
- Windows Hyper-V Server 2016;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2019 Core;
- Windows Storage Server 2019;
- Windows Hyper-V Server 2019.

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

- антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
- защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
- непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
- Анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- возможность проверки контейнеров Microsoft Windows;
- защита от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
- защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления;
- наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп);
- компонент создания специальных правил должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
- компонент создания специальных правил должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должен иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
- осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с

возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;

- осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем;
- информирование администратора о подключении внешних устройств;
- 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;
- наличие механизмов автоматической генерации правил для контроля устройств и приложений;
- 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.x;
- Red Hat Enterprise Linux 7.2 – 7.x;

- CentOS 6.7 и выше;
- Debian GNU / Linux 8.6 – 8.x;
- Debian GNU / Linux 9.4 - 9.x;
- Linux Mint 18.2 и выше;
- Linux Mint 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.x;
- Red Hat Enterprise Linux 7.2 – 7.x;
- CentOS 6.7 – 6.x;
- CentOS 7.2 – 7.x;
- Debian GNU / Linux 8.6 – 8.x;
- Debian GNU / Linux 9.4 - 9.x;
- OracleLinux 7.3 и выше;
- SUSE Linux Enterprise Server 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;
- Amazon Linux AMI;
- Linux Mint 18.2 и выше;
- Linux Mint 19 (последняя версия);
- Micro Focus Open Enterprise Server 2018;
- Astra Linux Special Edition 1.5 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
- Astra Linux Special Edition 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.

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

- резидентного антивирусного мониторинга;
- облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- проверку ресурсов доступных по SMB / NFS;
- эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;
- проверку сообщений электронной почты в текстовом формате (Plain text);
- наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
- защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
- 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;
- Apple iOS 10.0 – 12.

Программные средства для антивирусной защиты смартфонов для ОС Android должны обеспечивать следующую функциональность:

- 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 Firebase Cloud Messaging (FCM);
- базовая поддержка Android for Work;
- 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 (factory reset);
- 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.

Программные средства для антивирусной защиты смартфонов для ОС Apple iOS должны обеспечивать следующую функциональность, в том числе и с установленным плагином управления:

- возможность удаленной настройки параметров iOS MDM-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 Exchange ActiveSync\ iOS MDM;
- 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 supervised mode;

– возможность централизованного управления с помощью единой консоли управления.

Требования к программным средствам антивирусной защиты виртуальных сред с использованием агентов

Программные средства для антивирусной защиты должны функционировать под управлением следующих гипервизоров:

– VMware ESXi 6.0, 6.5, 6.7;
– Windows Server 2012 R2;
– Windows Server 2016;
– Windows Server 2019
– Citrix XenServer 7.1;
– Платформа Proxmox VE: гипервизор Proxmox VE 5.4;
– Huawei FusionSphere – FusionCompute CNA 6.3.1;
– Скала-Р 7.0.6;
– KVM на базе одной из следующих операционных систем:
– Ubuntu Server 16.04 LTS;
– Ubuntu Server 18.04 LTS;
– Red Hat Enterprise Linux Server 7,6;
– CentOS 7.6;

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

– Windows 7
– Windows 8.1
– Windows 10
– Windows Server 2008 R2
– Windows Server 2012
– Windows Server 2012 R2
– Windows Server 2016
– Windows Server 2019
– Debian GNU / Linux 8.11, 9.8
– Ubuntu Server 16.04, 18.04
– CentOS 6.10, 7,6
– Red Hat Enterprise Linux Server 6.10, 7.6, 8
– SUSE Linux Enterprise Server 15
– ALT Linux 8 (64-разрядная)
– ALT Linux 7.0.6 (64-разрядная)
– Oracle Linux 7.6 (64-разрядная)
– Astra Linux SE 1.6 (без поддержки режимов Мандатного разграничения доступа и Замкнутой программной среды)
– Astra Linux SE 1.5 (без поддержки режимов Мандатного разграничения доступа и Замкнутой программной среды)

Программные средства антивирусной защиты виртуальных сред должны обеспечивать реализацию следующих функциональных возможностей на настольных операционных системах Windows:

- резидентный антивирусный мониторинг;
- эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
- выполнение антивирусного сканирования и других ресурсоемких задач не на гостевых машинах, а на отдельной машине защиты;
- автоматическое обнаружение и подключение агентов на ВМ к функционирующей машине защиты, в том числе находящейся на другом хосте, в случае недоступности основной машины защиты.
- обеспечение непрерывности файловой защиты в период кратковременной недоступности машины защиты посредством журналирования всех файловых операций на защищаемой гостевой машине в период недоступности машины защиты, и выполнение автоматического сканирования всех изменений после восстановления доступа.
- облачная защита от новых угроз, позволяющая приложению при сканировании в режиме реального времени и в режиме запланированной проверки обращаться к специальным ресурсам производителя, для получения вердикта по файлу.
- защита электронной корреспонденции от вредоносных программ с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 — независимо от используемого почтового клиента.
- почтовый плагин для клиента Outlook с возможностью включения/отключения проверки вложений, а также возможностью удаления вложения или изменения формата вложенного файла.
- защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, HTTPS, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных сайтов.
- блокировка баннеров и всплывающих окон загружаемых с Web-страниц.
- распознавание и блокировка фишинг-сайтов.
- защита от еще не известных вредоносных программ на основе анализа их поведения.
- возможность определения аномального поведения приложения с помощью анализа действий этого приложения. Возможность совершить откат действий вредоносного программного обеспечения при лечении.
- защита от внешнего шифрования общих файлов и папок.
- возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы.
- наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп);
- компонент создания специальных правил должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме MD5 или SHA256;
- компонент создания специальных правил должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должен иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
- наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ

- защита от хакерских атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные.
- осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из AD.
- осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки определенного типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из AD.
- возможность проверки всех виртуальных машин по заранее заданному расписанию.
- предотвращение повторного сканирования уже проверенных файлов.
- наличие информации о проверенных файлах на машине защиты, позволяющей исключить повторную проверку одних и тех же файлов, находящихся на разных виртуальных машинах.
- блокирование, обезвреживание и удаление вредоносного ПО, уведомление администраторов.
- единая консоль управления для всех компонентов защиты
- консоль централизованного управления, единая для виртуальных сред и физических рабочих станций.
- возможность применять различные параметры безопасности для отдельных групп виртуальных машин.
- хранение резервных копий удаленных файлов.
- поддержка отката антивирусных баз.
- поддержка схемы лицензирования по числу защищаемых виртуальных машин (рабочие станции) и по количеству физических ядер CPU.
- механизм профилирования настроек антивируса, позволяющий дополнительно ограничить область ее применения.

Программные средства антивирусной защиты виртуальных сред должны обеспечивать реализацию следующих функциональных возможностей на серверных операционных системах Windows:

- резидентный антивирусный мониторинг.
- защита от программ-маскировщиков, программ автодозвона на платные сайты.
- эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.
- выполнение антивирусного сканирования и других ресурсоемких задач не на гостевых машинах, а на отдельной машине защиты;
- защита электронной корреспонденции от вредоносных программ с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 — независимо от используемого почтового клиента.
- автоматическое обнаружение и подключение к функционирующей машине защиты, в том числе находящейся на другом хосте, в случае недоступности основной машины защиты.
- обеспечение непрерывности файловой защиты в период кратковременной недоступности

машины защиты посредством журналирования всех файловых операций на защищаемой гостевой машине в период недоступности машины защиты, и выполнение автоматического сканирования всех изменений после восстановления доступа.

- облачная защита от новых угроз, позволяющая приложению при сканировании в режиме реального времени и в режиме запланированной проверки обращаться к специальным ресурсам производителя, для получения вердикта по файлу.
- защита от еще не известных вредоносных программ на основе анализа их поведения.
- Защита от внешнего шифрования общих файлов и папок.наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ
- защита от хакерских атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные.
- централизованные обновления с возможностью хранения части антивирусных баз на машине защиты
- возможность проверки всех виртуальных машин по заранее заданному расписанию.
- предотвращение повторного сканирования уже проверенных файлов.
- наличие информации о проверенных файлах на машине защиты, позволяющей исключить повторную проверку одних и тех же файлов, находящихся на разных виртуальных машинах.
- блокирование, обезвреживание и удаление вредоносного ПО, уведомление администраторов.
- единая консоль управления для всех компонентов защиты
- консоль централизованного управления, единая для виртуальных сред и физических рабочих станций.
- предоставление подробной информации о событиях на виртуальных машинах и о выполнении задач.
- возможность применять различные параметры безопасности для отдельных групп виртуальных машин.
- хранение резервных копий удаленных файлов.
- поддержка отката антивирусных баз.
- поддержка схемы лицензирования по числу защищаемых виртуальных машин (сервера), по количеству физических ядер CPU.
- механизм профилирования настроек антивируса, позволяющий дополнительно ограничить область ее применения.

Программные средства антивирусной защиты виртуальных сред должны обеспечивать реализацию следующих функциональных возможностей на серверных операционных системах Linux:

- резидентный антивирусный мониторинг;
- эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;

- проверка сообщений электронной почты в текстовом формате (Plain text);
- наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
- помещение подозрительных и поврежденных объектов на карантин;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
- сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
- поддержка файловой системы GlusterFS на виртуальных машинах с установленным Легким агентом для Linux;
- возможность проверки загрузочных секторов, системной памяти и объектов автозапуска.

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 R2 32-разрядная / 64-разрядная;
- Windows Server 2012, 2012 R2 64-разрядная;
- Windows Server 2016 64-разрядная.

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;
- Oracle VM VirtualBox 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;

- Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная;
- Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная;
- Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная;
- Microsoft SQL Server 2012 (все редакции) 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft 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;
- MySQL Enterprise 5.7 32-разрядная / 64-разрядная.

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

- 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 поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети;
- автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети;
- возможность настройки правил переноса обнаруженных компьютеров 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 ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
- возможность иерархии триггеров по которым происходит перераспределение;
- автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
- тестирование загруженных обновлений средствами ПО централизованного управления

перед распространением на клиентские машины;
- доставка обновлений на рабочие места пользователей сразу после их получения;
- распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
- построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
- наличие преднастроенных ролей пользователей средств централизованного управления;
- должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей;
- 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;
- возможность подключения по RDP или штатными средствами из консоли управления;
- пользователю должен выводиться запрос на разрешение дистанционного подключения;
- наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
- 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" (bare metal);
- 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 (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры
- 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;
- поддержка функциональности управления шифрованием данных;
- 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;
- портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотра мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
- наличие системы контроля возникновения вирусных эпидемий;
- возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF.
- 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 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.

Программное обеспечение должно поставляться Заказчику на цифровых носителях в следующем составе:

- комплект файлов, необходимых для установки системы и работы пользователя;

Раздел 4. Место выполнения работ и оказания услуг с указанием конкретного адреса.

Юридический адрес Заказчика:

210100, Республика Узбекистан, город Навои, улица Инспекторов 7. По условиям настоящего технического задания транспортные расходы по прибытию в город Навои и расходы на проживание сотрудников Исполнителя в городе Навои на период выполнения услуги будут понесены самим Исполнителем.

Объект расположен на территории Навоийской области. При этом расходы на транспортировку Исполнителя до мест дислокации объекта берет на себя Заказчик.

Раздел 5. Условия выполнения работ и оказания услуг.

Допущения и ограничения:

- Заказчик обязуется сохранять конфиденциальность информации о деятельности Исполнителя, полученной им для услуг в соответствии с Договором;
- Исполнитель обязуется сохранять конфиденциальность информации о деятельности Заказчика, полученной им для оказания услуг в соответствии с Договором;
- Заказчик обязуется назначить из числа своих работников лицо (лица), ответственные за организацию оказания услуг со стороны Заказчика и решение с Исполнителем оперативных вопросов, возникших в ходе исполнения Сторонами обязательств (создание рабочих групп, выделенных необходимых ресурсов со стороны Заказчика, участие в обсуждениях, согласование требований других сотрудников Заказчика и др.). При этом у назначенного работника (работников) должны быть полномочия давать обязательные для выполнения распоряжения всем задействованным в проекте сотрудникам Заказчика. Руководитель проекта должен иметь возможность уделять не менее 20% рабочего времени вопросам управления проектом;
- В случае передачи Исполнителю на любых носителях информации, содержащей персональные данные, обезличить персональные данные. Исполнитель не несет ответственности за персональные данные Заказчика, и не обрабатывает персональные данные Заказчика;

Раздел 6. Требования к исполнителю работ исходя из сложности выполняемых работ и оказываемых услуг, разработанные и утвержденные в установленном порядке.

Исполнитель должен иметь репутацию, достаточный опыт реализации проектов сопоставимого уровня, в том числе, международных, а также необходимые сертификаты и ресурсы, позволяющие выполнить задание на требуемом уровне, дающем основания полагать, что внедренная информационная система будет принята.

Исполнитель должен соответствовать следующим обязательным требованиям:

– иметь опыт в соответствующих по масштабу проектах;

– иметь соответствующие разрешительные документы (лицензии и сертификаты) для специалистов, принимающих участие в проекте;

– отсутствие в отношении участника открытого конкурса фактов проведения процедуры ликвидации, а также решений арбитражного суда о признании участника открытого конкурса банкротом;

– исполнитель не вправе осуществлять действия, влекущие возникновение конфликта интересов или создающие угрозу возникновения такого конфликта.

Раздел 7. Сроки (периоды) выполнения работ и оказания услуг (график выполнения работ).

Сроки поставки ПО: в течение 10 дней после подписания договора.

Раздел 8. Требования к безопасности выполнения работ и оказания услуг и их результатов.

– Программное обеспечение должно соответствовать по надёжности международным стандартам, стандартам и техническим регламентам Республики Узбекистан, которые относятся к данной отрасли.

– Программное обеспечение должно соответствовать по безопасности международным стандартам, стандартам и техническим регламентам Республики Узбекистан, которые относятся к данной отрасли.

Для обеспечения сохранности информации в системе должны быть включены следующие функции:

– техническое обслуживание заключается в осуществлении технической поддержки и обновлении программного обеспечения, которые должны осуществляться в рамках оформляемого контракта в течение 2 лет. Последующее обновление будет производиться по необходимости.

Раздел 9. Порядок сдачи и приёмки результатов работ и услуг

Оказанные услуги Исполнитель оформляет актом выполненных работ (услуг) согласно проекту, согласовывает с Заказчиком и предоставляет Заказчику счет-фактуру на сумму выполненных работ (услуг) и двухсторонне оформленные акты выполненных работ (услуг) по проекту.

Раздел 10. Требования по передаче технических и иных документов по завершению и сдаче результатов работ и услуг.

По завершению работ Исполнитель передает Заказчику следующие документы:

- руководство администратора серверного программного обеспечения в соответствии с действующими в Республике Узбекистан стандартами;
- руководство пользователя в соответствии с действующими в Республике Узбекистан стандартами;
- руководство администратора базы данных в соответствии с действующими в Республике Узбекистан стандартами;

Раздел 11. Требования по техническому обучению исполнителем персонала заказчика по результатам выполненных работ и оказанных услуг.

Обучение персонала не требуется

Раздел 12. Требования по объёму гарантий качества работ и услуг

Разработанная система должна отвечать требованиям следующих нормативных и распорядительных документов:

- O‘zDSt 1986:2018 Информационная технология. Информационные системы. Стадии создания;
- O’zDst 1985:2018 Информационная технология. Виды, комплектность и обозначение документов при создании информационных систем.

Раздел 13. Требования об указании срока гарантий качества на результаты работ и услуг.

В соответствии с требованиями законодательства Республики Узбекистан.

Раздел 14. Авторские права с указанием условий о передаче исключительных прав на объекты интеллектуальной собственности, возникших в связи с исполнением обязательств исполнителя по выполнению работ и оказанию услуг.

После ввода системы в эксплуатацию, Исполнитель передает полные права на пользование и владение программным обеспечением (на электронных носителях информации).

Требования к патентной и лицензионной чистоте: ПО должно состоять из экземпляров, которые распространяются и используются в объёмах и на условиях, определённых в лицензиях.

Раздел 15. Иные требования к работам

Требования по стандартизации и унификации

При эксплуатации системы должны использоваться технические средства, операционные системы, системы управления базами данных, позволяющих построить единое информационное пространство в рамках комбината и обеспечивающих прозрачность доступа к данным.

Стандартизация и унификация технических средств системы должна обеспечиваться посредством использования серийно выпускаемых средств вычислительной техники и коммуникационного оборудования.

Ответственный исполнитель

/Начальник ЦИКТ _____ **С.Г. Ганиев**
(подпись, дата)

Соисполнители

Руководитель группы Р и А по ЦИКТ _____ **С.Н. Нарзуллаев**
(подпись, дата)

Нормоконтроль Заместитель начальника ЦИКТ _____ **Б.Ф. Носиров**
(подпись, дата)