

«УТВЕРЖДАЮ»
Генеральный директор
АО «Гидропроект»

Р. Н. Орищук

« 11 » ноября 2022 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Техническое задание на продление лицензии на антивирусное
программное обеспечение

на 19 листах

действует с 11.11.2022

«СОГЛАСОВАНО»

Директор по экономике и финансам
Н.Н. Тураев

« 11 » ноября 2022 г.

«РАЗРАБОТАНО»

Начальник отдела информационно-
коммуникационных технологий
У.Э. Инагамджанов

« 11 » ноября 2022 г.

г. Ташкент

Содержание

Спецификация поставляемого товара	2
Общие требования.....	2
Требования к программным средствам антивирусной защиты для рабочих станций Windows.....	2
Требования к программным средствам антивирусной защиты для серверов Windows	5
Требования к программным средствам антивирусной защиты для рабочих станций Mac.....	6
Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux	7
Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows	9
Требования к программным средствам антивирусной защиты мобильных устройств.....	12
Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows.....	13
Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux.....	17
Требования к обновлению антивирусных баз	18
Требования к эксплуатационной документации	19
Требования к технической поддержке	19

Спецификация поставляемого товара

Описание позиции	Количество защищаемых объектов	Срок действия лицензии, год
Неисключительные права на использование	300	3

Общие требования

Антивирусные средства должны включать:

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

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

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

Требования к программным средствам антивирусной защиты для рабочих станций Windows

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

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше;
- Windows 8 Professional / Enterprise (32 / 64-разрядная);
- Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
- Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise;
- Windows 11.

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, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
- фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
- проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
- блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
- распознавания и блокировку фишинговых и небезопасных сайтов;
- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
- 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;

- 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;

- назначение приоритета для правил доступа к устройствам с файловой системой;

- контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;

- защиты от атак типа BadUSB;

- запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

- защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;

- управления параметрами через доверенные программы удаленного администрирования;

- установки только выбранных компонентов программного средства антивирусной защиты;

- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

- запуска 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;

- проверки целостности антивирусной программы;

- добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;

- импорта и экспорта списков правил и исключений в XML-формат;

- наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

- наличие защищенного хранилища для отчетов о работе антивируса;

- включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;

- интеграции с Windows Defender Security Center;

- наличие поддержки Antimalware Scan Interface (AMSI);

- наличие поддержки Windows Subsystem for Linux (WSL);

- защитить паролем восстановление объектов из резервного хранилища;

- ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;

- наличие инструмента мониторинга сети по протоколам TCP и UDP;

- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
- возможность установки ограничения длительности выполнения задачи.

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 2011 Essentials / Standard (64-разрядная), Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2;
- Windows MultiPoint Server 2011 (64-разрядная);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

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;
- 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;

- защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;

- 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;

- проверки целостности антивирусной программы;

- 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;

- включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;

- интеграции с Windows Defender Security Center;

- наличие поддержки Antimalware Scan Interface (AMSI);

- наличие поддержки Windows Subsystem for Linux (WSL);

- защитить паролем восстановление объектов из резервного хранилища.

- импорта и экспорта списков правил и исключений в XML-формат;

- ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;

- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;

- возможность установки ограничения длительности выполнения задачи;

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 10.14 - 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;
- возможность установки расширений из командной строки с помощью новой команды kav.

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 32-битных операционных систем следующих версий:

- CentOS 6.7 и выше.
- Debian GNU / Linux 9.4 и выше.
- Debian GNU / Linux 10.1 и выше.
- Debian GNU / Linux 11.1 и выше.
- Linux Mint 19 и выше.
- Mageia 4.
- Red Hat Enterprise Linux 6.7 и выше.
- Альт Образование 9.
- Альт Рабочая Станция 9.
- Альт Сервер 9.

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

- AlterOS 7.5 и выше.
- Amazon Linux 2.
- Astra Linux Common Edition (очередное обновление 2.12).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
- 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.
- Debian GNU / Linux 11.1 и выше.
- EulerOS V2.0SP2 2.2.17.
- EulerOS V2.0SP5 2.5.6.
- Linux Mint 19 и выше.
- Linux Mint 20.1 и выше.
- openSUSE Leap 15.0 и выше.
- Oracle Linux 7.3 и выше.
- Oracle Linux 8.0 и выше.
- Pardus OS 19.1.
- Red Hat Enterprise Linux 6.7 и выше.
- Red Hat Enterprise Linux 7.2 и выше.
- Red Hat Enterprise Linux 8.0 и выше.
- SUSE Linux Enterprise Server 12 SP5 и выше.
- SUSE Linux Enterprise Server 15 и выше.
- Ubuntu 18.04 LTS и выше.
- Ubuntu 20.04 LTS.
- Альт Образование 9.
- Альт Рабочая Станция 9.
- Альт Сервер 9.
- Гослинукс 7.2.
- РЕД ОС 7.3.

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 проверку 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 информации о проверенных и не измененных после проверки файлах);
- защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
- включения опции блокирования файлов во время проверки;
- помещение подозрительных и поврежденных объектов на карантин;
- 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;
- 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;
- управления через пользовательский графический интерфейс без root прав;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;
- управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;
- проверки съемных дисков;
- отслеживания во входящем сетевом трафике активности, характерной для сетевых атак
- проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым;
- получения данных о действиях программ на компьютере пользователя;
- создание файлов трассировки при запуске программы.

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 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 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 SP2 или выше;
- Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
- Microsoft Small Business Server 2008 Standard / Premium SP2 или выше;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
- Windows Server 2008 R2 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 SP1 или выше;
- Microsoft Windows MultiPoint Server 2011 Standard / Premium;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
- Microsoft 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;
- Windows Server 2022;
- Windows 10 Enterprise multi-session.

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

- антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
 - запуск задач по расписанию и/или сразу после загрузки операционной системы;
 - облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
 - антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
 - защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
 - непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнения тех из них, которые признаются опасными.
 - анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
 - проверки контейнеров Microsoft Windows;
 - защиты от эксплуатации уязвимостей в памяти процессов;
 - должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
 - 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;
 - 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;
 - интеграции с SIEM системами;
 - указания количества рабочих процессов антивируса вручную;
 - отключить графический интерфейс;
 - наличие удаленной и локальной консоли управления;
 - управления параметрами антивируса из командной строки;
 - централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

- управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
- защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;
- включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.

Требования к программным средствам антивирусной защиты мобильных устройств

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

- Android 5.0-12.0.
- iOS 10.0-15.0 или iPadOS 13-15.

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

- постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;
- проверка файловой системы устройства по требованию и по расписанию;
- мгновенная проверка устанавливаемых приложений
- блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
- 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;
- отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);
- заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
- указать параметры подключения к wi-fi сетям;
- указать обязательные к установке приложения;
- блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);
- создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
- поддержка технологий Samsung KNOX1 и KNOX2.

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

- удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;
- отправки команды блокирования и удаления данных;
- 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;
- централизованного управления с помощью единой консоли управления;
- наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве.

Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows

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

- Microsoft Windows 11 Home 64-разрядная;
- Microsoft Windows 11 Pro 64-разрядная;
- Microsoft Windows 11 Enterprise 64-разрядная;
- Microsoft Windows 11 Education 64-разрядная;
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная / 64-разрядная;
- Microsoft Windows 10 20H2 32-разрядная / 64-разрядная;
- Microsoft Windows 10 20H1 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 2016 LTSC 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Enterprise 2015 LTSC 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;
- Microsoft Windows 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 Home 19H2 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro 19H2 32-разрядная / 64-разрядная;
- Microsoft Windows 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;
- Windows Server 2022 Standard 64-разрядная;
- Windows Server 2022 Core 64-разрядная;
- Windows Server 2022 Datacenter 64-разрядная;
- Windows Server 2019 Standard 64-разрядная;
- Windows Server 2019 Core 64-разрядная;
- Windows Server 2019 Datacenter 64-разрядная;
- Windows Server 2016 Standard (LTSC) 64-разрядная;
- Windows Server 2016 (вариант установки Server Core) (LTSC) 64-разрядная;
- Windows Server 2016 Datacenter (LTSC) 64-разрядная;
- Windows Server 2012 R2 Standard 64-разрядная;
- Windows Server 2012 R2 Server Core 64-разрядная;
- Windows Server 2012 R2 Foundation 64-разрядная;
- Windows Server 2012 R2 Essentials 64-разрядная;
- Windows Server 2012 R2 Datacenter 64-разрядная;
- Windows Server 2012 Standard 64-разрядная;
- Windows Server 2012 Server Core 64-разрядная;
- Windows Server 2012 Foundation 64-разрядная;
- Windows Server 2012 Essentials 64-разрядная;
- Windows Server 2012 Datacenter 64-разрядная;
- Windows Server 2008 R2 with Standard Service Pack 1 и выше 64-разрядная;
- Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;
- Windows Storage Server 2016 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Windows Storage Server 2012 64-разрядная.

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

- VMware vSphere 6.7;
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;

- Microsoft Hyper-V Server 2019 64-разрядная;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Parallels Desktop 17;
- Oracle VM VirtualBox 6.x (только гостевой вход Windows).

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

- Microsoft SQL Server 2012 Express 64-разрядная;
- Microsoft SQL Server 2014 Express 64-разрядная;
- Microsoft SQL Server 2016 Express 64-разрядная;
- Microsoft SQL Server 2017 Express 64-разрядная;
- Microsoft SQL Server 2019 Express 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;
- Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная;
- Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная (требуется дополнительные действия);
- Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуется дополнительные действия);
- MySQL 5.7 Community 32-разрядная / 64-разрядная;
- MySQL Standard Edition 8.0 32-разрядная / 64-разрядная;
- MySQL Enterprise Edition 8.0 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;
- MariaDB Galera Cluster 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;
- чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
- 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;

- 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;

- 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;

- отправки SMS-оповещений о заданных событиях;

- централизованная установка сертификатов на управляемые мобильные устройства;

- указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;

- 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 карантинных ресурсов 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 портала самообслуживания пользователей;
- портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
- наличие системы контроля возникновения вирусных эпидемий;
- установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
- интеграции по OpenAPI;
- управления антивирусной защитой с использованием WEB консоли;
- двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
- использования дополнительной аутентификация после изменения параметров учетной записи пользователя.
- возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами;
- возможность развернуть сервер администрирования как систему высокой доступности.

Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux

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

- Ubuntu 18.04 LTS;
- Ubuntu 20.04 LTS;
- Debian GNU / Linux 10.5;
- Astra Linux Common Edition, версия 2.12;
- Astra Linux Special Edition, версия 1.6;
- CentOS 7.9.2009;
- CentOS 8.3.2011;
- Red Hat Enterprise Linux 7.9;
- Red Hat Enterprise Linux 8.3;
- ALT 8.3;
- ALT 9.1.

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

- FusionCompute 8.0;
- FusionSphere OpenStack 6.5.13.

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

• MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB, MySQL 8.0 32-разрядная / 64-разрядная.

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

- централизованные установка, обновление и удаление программных средств антивирусной защиты;
- централизованная настройка, администрирование;
- просмотр отчетов и статистической информации по работе средств защиты;
- сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
- иерархии триггеров, по которым происходит перераспределение;
- 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;
- наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
- построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;
- наличие предустановленных стандартных отчетов о работе системы;
- экспорт отчетов в файлы форматов PDF и XML;
- централизованное управление объектами резервных хранилищ и карантин 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;
- наличие системы контроля возникновения вирусных эпидемий;
- управления антивирусной защитой с использованием WEB консоли;

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

- создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток;
- множественность путей обновления, в том числе — по каналам связи и на отчуждаемых электронных носителях информации;
- проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

- «Руководство пользователя (администратора)»

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

- Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Республики Узбекистан по электронной почте и через Интернет.
- Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.