

Техническая спецификация по продлению лицензии на имеющееся программное обеспечение по антивирусной защите рабочих станций и серверов.

П/п.: 81512296

Антивирусная защита (АЗ) должна представлять собой корпоративное решение, обеспечивающее устойчивое функционирование в сети рабочих станций и серверов. В рамках всей организации используются единые антивирусные средства. Настоящая Техническая спецификация является основополагающим документом, устанавливающим требования к поставляемому программному обеспечению с оказанием сопутствующих услуг по внедрению системы антивирусной защиты. Все компоненты системы имеют полную интеграцию между собой.

Общие требования к программному обеспечению по антивирусной защите

Наименование имеющегося программного обеспечения: Kaspersky Endpoint Security for Business Advanced License - 723 лицензий.

Срок действия лицензии: не менее 12 месяцев с момента генерации лицензий на программное обеспечение.

Срок поставки: не более 15 календарных дней со дня вступления договора в законную силу.

Антивирусные средства должны включать:

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

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

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

Требования к программным средствам антивирусной защиты для рабочих станций Windows

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

- Windows 7 Home / Professional / 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/Enterprise multi-session;
- Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise;
- Windows 11 для Arm64 Home / Pro / Pro для рабочих станций / Education / Enterprise.

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;
- формировать область защиты для функции защиты папок общего доступа от внешнего шифрования;
- 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;
- 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;
- установки ограничение длительности выполнения задачи;
- возможность ставить задачи проверки в очередь, если проверка уже выполняется;
- обновление без перезагрузки системы;
- настроить доступ пользователей к мобильным устройствам в приложении Android Debug Bridge (ADB);
- заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству запрещен;
- настроить права печати для пользователей;
- наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi;
- наличие совместимости с Azure WVD;
- настроить доступ пользователей к мобильным устройствам в приложении iTunes;
- запуск специальной задачи для обнаружения и закрытия 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;
- возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий)
- возможность создавать служебную учетную запись агента аутентификации при шифровании диска;
- поддержка стороннего поставщика учетных данных ADSelfService Plus для работы SSO при полнодисковом шифровании;
- возможность настроить исключения и ограничить доступ ко всем Bluetooth-устройствам кроме устройств ввода;
- возможность обновления приложения без перезагрузки операционной системы;
- возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО;
- возможность запретить внешнее управление службами приложения;
- возможность выбирать предустановленные исключения из проверки и доверенные приложения;
- возможность задать разрешение отдельному пользователю на экспорт настроек в конфигурационный файл;
- возможность мониторинга и отзыва временных паролей на доступ к приложению, позволяющий сохранять историю паролей (до 30 дней) и контролировать статус (Активен, Истек, Отзыван);
- возможность разрывать подключение к веб-ресурсам, запрещенными правилами Веб-Контроля, сразу после применения политики;
- возможность настраивать разные наборы компонентов для разных типов операционных систем в инсталляционном пакете;
- возможность выбирать предустановленные исключения из проверки и доверенные приложения;
- возможность блокировать сетевые соединения по устаревшему протоколу TLS 1.0;
- поддержка протокола Kerberos для аутентификации приложения через прокси-сервер для доступа в интернет;
- возможность указывать хеш файла для исключения приложения из проверки.

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 Web Server 2008 R2 Service Pack 1 и выше;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2016 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (включая режим Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая режим Server Core).
- Windows Server 2025 Standard / Datacenter.

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;
- 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;

- 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 и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
- поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов.
- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
- возможность установки ограничения длительности выполнения задачи;
- возможность ставить задачи проверки в очередь, если проверка уже выполняется;
- обновление без перезагрузки системы;
- настройки прав доступа (чтение / запись) для портативных устройств (MTP), выбирать пользователей или группу пользователей, которые имеют доступ к устройствам, а также задавать расписание доступа к устройствам;
- заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству запрещен;
- настроить права печати для пользователей;
- наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi;
- наличие совместимости с Azure WVD;
- возможность обновления приложения без перезагрузки операционной системы;
- возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО.
- возможность запретить внешнее управление службами приложения.
- возможность использования предустановленных исключений из проверки и доверенных приложений, предназначенных для быстрой настройки доверенной зоны для работы приложения на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager;
- поддержка протокола Kerberos для аутентификации приложения через прокси-сервер для доступа в интернет;
- возможность указывать хеш файла для исключения приложения из проверки.

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 12 - 15;

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;
- задавать исключения при проверке указанных областей на уровне перехватов файловых операций;
- автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены;
- ограничивать загрузку процессора приложением при выполнении задач поиска вредоносного ПО;
- включения облачного режима и использования облегченной версии баз вредоносного ПО, для снижения нагрузки на ресурсы операционной системы;
- пропускать сканирование системного тома, доступного только для чтения, во время выполнения задач проверки по требованию;
- анализа активности приложений в операционной системе с использованием шаблонов опасного поведения (BSS);
- установки из файла .pkg через JAMF;
- автоматического сканирования внешних дисков при их подключении;
- поддержки клиентских сертификатов;
- проверки вложений входящих и исходящих сообщений электронной почты на наличие в них вредоносного ПО и других угроз;
- управления доступом пользователей к установленным или подключенным к компьютеру устройствам;
- блокировки несанкционированных подключений к компьютеру во время работы в интернет или локальной сети и контроль сетевой активности приложений;
- откат действий вредоносного программного обеспечения, связанных с его файловой, системной или сетевой активностью в ОС;
- защита от эксплойтов.
- централизованного управления всеми вышеуказанными компонентами с помощью единой системы управления.

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:

- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12

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

- AlmaLinux OS 8.6, 8.7, 8.8, 8.9.
- AlmaLinux OS 9.4, 9.5, 9.6.
- AlterOS® 2025.
- Amazon™ Linux 2023.
- Astra Linux Common Edition 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.10015-01 (очередное обновление 1.7).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8).
- Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6).
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3).
- Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7).
- CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- CentOS Stream 8.
- CentOS Stream 9.
- CentOS Stream 10.
- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12.
- Debian GNU/Linux 13.0, 13.1, 13.2.
- EMIAS 1.0.
- EulerOS 2.0 SP10.
- Fedora 41.
- Kylin 10.
- Linux Mint 21.3.
- Linux Mint 22.2.
- Mostech 12 release 2021.1.

- openSUSE Leap 15.6.
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9.
- Oracle Linux 9.4, 9.5, 9.6.
- Red Hat® Enterprise Linux® 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9.
- Red Hat Enterprise Linux 9.4, 9.5, 9.6.
- Red Hat Enterprise Linux 10.0, 10.1.
- Rocky Linux 8.6, 8.7, 8.8, 8.9.
- Rocky Linux 9.4, 9.5, 9.6.
- SberLinux 8.10, 9.1, 9.5, 9.6.
- SberOS 3.4.0, 3.5.0.
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7.
- SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7.
- Ubuntu® 22.04 LTS.
- Ubuntu 24.04 LTS.
- Альт Образование 10.
- Альт Образование 11.
- Альт Рабочая Станция 11.
- Альт Сервер 11.
- Альт СП Сервер релиз 10.
- Альт СП Рабочая Станция релиз 10.
- Атлант, сборка Alcyone, версия 2022.02.
- Гослинукс 7.2.
- МОС 12 Сервер release 2021.1.
- МосОС 15.5 Arbat.
- МСВСФЕРА 9.4 АРМ.
- МСВСФЕРА 9.4 СЕРВЕР.
- ОС МЭШ 12 Для всех пользователей (без телеметрии и без поддержки ДИТ) release 2021.1.
- ОС МЭШ 12 Для московских школ для интерактивных панелей (с телеметрией и поддержкой ДИТ) release 2021.1.
- ОС МЭШ 12 Для московских школ для компьютеров и ноутбуков (с телеметрией и поддержкой ДИТ) release 2021.1.
- ОСнова 2.14.
- ОСнова 3.0.5.
- РЕД ОС® 7.3.
- РЕД ОС 8.0.
- РОСА "Кобальт" 7.9 Рабочая станция.
- РОСА "Кобальт" 7.9 Сервер.
- РОСА "Хром" 12 Рабочая станция.
- РОСА "Хром" 12 Сервер.
- СинтезМ-Клиент 8.6.
- СинтезМ-Сервер 8.6.

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

- Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
- CentOS Stream 9.
- EulerOS 2.0 SP10.
- SUSE Linux Enterprise Server 15.
- Ubuntu 22.04 LTS.
- Альт СП Рабочая Станция релиз 10.
- Альт СП Сервер релиз 10.
- РЕД ОС 8.0.

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 входящих и исходящих сообщений электронной почты;
- 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;
- получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация);
- создание файлов трассировки при запуске программы;
- получение информации обо всех исполняемых файлах программ, установленных на компьютерах;
- проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;
- сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий;
- исключения процессов из проверки памяти процессов в общих параметрах программы;
- оптимизировать проверку журналов работы программ с помощью параметра SkipPlainTextFiles;
- исключения трафика из проверки программой;
- использовать формат JSON для запросов и вывода информации, а также для экспорта и импорта параметров программы и параметров задач;
- установки и работы на устройствах с операционными системами для архитектуры Arm;
- работать в режиме информирования пользователя в случае обнаружения угроз или при обнаружении попытки доступа к устройству;
- возможность управлять запуском приложений на защищаемых устройствах с помощью правил контроля в режимах списка запрещенных или разрешенных приложений;
- автоматический перезапуск приложения при обновлении;
- возможность задать ограничение на использование ресурсов процессора;
- возможность в автоматическом режиме выключить компоненты защиты и задачи проверки при запуске приложения после установки;
- уведомления пользователя о работе компонентов и задач в графическом пользовательском интерфейсе;
- возможность читать память процессов, не останавливая их (ядра Linux начиная с версии 3.4);
- возможность управлять доступом пользователей к веб-ресурсам;
- возможность управлять запуском приложений на защищаемых устройствах;
- функция мониторинга стабильности собственной работы приложения;
- защита от эксплойтов с возможностью настройки исключения объектов из проверки;
- возможность настроить список пользователей или групп пользователей контроля устройств, для которых добавленные устройства будут доверенными;
- возможность разрешать доступ к устройствам хранения данных только на чтение;

- возможность настраивать исключения для отдельных компонентов приложения при использовании прокси-сервера;
- возможность настраивать исключения из перехвата трафика;
- возможность временного исключения из проверки файлов журналов баз данных;
- возможность экспорта и импорта списков исключений в политиках и задачах, применяемых к приложению;
- возможность настраивать отмену запуска запланированных задач на устройстве, работающем от аккумулятора;
- возможность вывода списка функций приложения в командной строке, информацию об их статусах (используется или не используется) и технологиях Linux, с помощью которых реализованы эти функции приложения;
- возможность защиты от атак типа BadUSB;
- возможность отображать в командной строке и в графическом интерфейсе информацию о действующей на устройстве политике и профилях политики.

Требования к программным средствам антивирусной защиты мобильных устройств

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

- Android 5.0 и выше (включая Android 12L, исключая Go Edition);
- iOS 15 и выше или iPadOS 15 и выше;

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;
- указать разрешенные версии приложений при создании правил Контроля приложений для Android-устройств.

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.
- запретить изменение настроек Bluetooth для iOS MDM-устройств

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:

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSC) 64-разрядная.
- Windows Server 2019 Standard/Datacenter/Core 64-разрядная.
- Windows Server 2022 Standard/Datacenter/Core 64-разрядная.
- Windows Server 2025 Standard/Datacenter/Core 64-разрядная.
- Windows Storage Server 2019 64-разрядная.

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

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- Microsoft Hyper-V Server 2019 64-разрядная.
- Microsoft Hyper-V Server 2022 64-разрядная.
- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- Parallels Desktop 18.
- Oracle VM VirtualBox 7.x.

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

- Microsoft SQL Server 2016 (все редакции) 64-разрядная.
- Microsoft SQL Server 2017 (все редакции) для Windows/Linux 64-разрядная.
- Microsoft SQL Server 2019 (все редакции) для Windows/Linux 64-разрядная (требуется дополнительные действия).
- Microsoft SQL Server 2022 (все редакции) для Windows/Linux 64-разрядная.
- MySQL 5.7 Community 32-разрядная/64-разрядная.
- MySQL 8.0 Community 32-разрядная/64-разрядная.
- MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- PostgreSQL 13.x 64-разрядная.
- PostgreSQL 14.x 64-разрядная.
- PostgreSQL 15.x 64-разрядная.
- Postgres Pro 13.x Windows/Linux 64-разрядная.
- Postgres Pro 14.x Windows/Linux 64-разрядная.

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

- выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
- 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 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 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 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;
- возможность управления развертыванием ОС Windows через консоль управления;
- 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;
- возможность подключения по RDP или штатными средствами из консоли управления;
- наличие возможности совместного подключения к рабочему столу Windows (Windows Desktop Sharing);
- пользователю должен выводиться запрос на разрешение дистанционного подключения;
- наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (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;
- поддержка функциональности управления шифрованием данных;
- возможность интеграции с SIEM системами и передача событий в формате syslog или CEF/LEEF

- 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.
- автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей и серверах под управлением Microsoft Windows;
- возможность развернуть Сервер администрирования как систему высокой доступности;
- возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети.
- удаленная диагностика клиентских устройств на базе Windows и Linux (получение трассировок, журналов событий, дампов, остановка и запуск приложений);
- возможность отозвать права локального администратора учетных записей на управляемых устройствах с операционной системой Linux;
- возможность изменить пароль локальной учетной записи на управляемых устройствах с операционной системой Linux.

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:

- Debian GNU/Linux 12 (Bookworm) 64-разрядная.
- Debian GNU/Linux 13 (Trixie) 64-разрядная.
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
- Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная.
- CentOS Stream 9 64-разрядная.
- CentOS Stream 10 64-разрядная.
- Red Hat Enterprise Linux Server 7.x 64-разрядная.
- Red Hat Enterprise Linux Server 8.x 64-разрядная.
- Red Hat Enterprise Linux Server 9.x 64-разрядная.
- Red Hat Enterprise Linux Server 10.x 64-разрядная.
- SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная.
- SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядная.
- Astra Linux Special Edition RUSB.10015-03 (очередное обновление 7.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядная.
- Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
- Альт СП Сервер 10 64-разрядная.
- Альт СП Рабочая станция 10 64-разрядная.
- Oracle Linux 7 64-разрядная.
- Oracle Linux 8 64-разрядная.
- Oracle Linux 9 64-разрядная.
- Platform V SberLinux OS Server (SLO) 8.10.1 64-разрядная.
- Platform V SberLinux OS Server (SLO) 9.5.1 64-разрядная.
- Platform V SberLinux OS Server (SLO) 9.6 64-разрядная.
- РЕД ОС 7.3 Сервер 64-разрядная.
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
- РЕД ОС 8 64-разрядная.
- РОСА "КОБАЛЬТ" 7.9 64-разрядная.
- М ОС (Moscow Electronic School) 12 Сервер 64-разрядная.
- Mostech Server 64-разрядная.
- MocOC 15.5 Arbat 64-разрядная.

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

- VMware vSphere 6.7.0.
- VMware vSphere 7.0.3.
- Microsoft Hyper-V Server 2019 64-разрядная.

- Microsoft Hyper-V Server 2022 64-разрядная.
- Citrix XenServer 7.x.
- Citrix XenServer 8.2.
- Parallels Desktop 18.
- Oracle VM VirtualBox 7.0.12.
- Kernel-based Virtual Machine (все поддерживаемые ОС Linux).

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

- MySQL 5.7 Community 32-разрядная/64-разрядная.
- MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
- MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
- MySQL Standard Edition 8.4 32-разрядная/64-разрядная.
- MySQL Enterprise Edition 8.4 32-разрядная/64-разрядная.
- MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.4 (сборка 10.4.20 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.5 (сборка 10.5.27 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.6 (сборка 10.6.20 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.11 (сборка 10.11.10 и выше) 32-разрядная/64-разрядная.
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- PostgreSQL 13.x 64-разрядная.
- PostgreSQL 14.x 64-разрядная.
- PostgreSQL 15.x 64-разрядная.
- PostgreSQL 15.x 64-разрядная (кластер Corosync/Pacemaker).
- PostgreSQL 16.x 64-разрядная.
- PostgreSQL 17 64-разрядная.
- PostgreSQL 18 64-разрядная.
- Postgres Pro 13.x (все редакции) 64-разрядная.
- Postgres Pro 14.x (все редакции) 64-разрядная.
- Postgres Pro 15.x (все редакции) 64-разрядная.
- Postgres Pro 15.x 64-разрядная (кластер Corosync/Pacemaker).
- Postgres Pro 16.x (все редакции) 64-разрядная.
- Postgres Pro 16.x Enterprise 64-разрядная (кластер Built-in High Availability).
- Postgres Pro 17 (все редакции) 64-разрядная.
- Postgres Pro 17 Enterprise 64-разрядная (кластер Built-in High Availability).
- Postgres Pro 18 (все редакции) 64-разрядная.
- Postgres Pro 18 Enterprise 64-разрядная (кластер Built-in High Availability).
- Platform V Pangolin 6.5.1 64-разрядная.
- Platform V Pangolin 6.5.1 64-разрядная (кластер Built-in High Availability).
- Jatoba 4 64-разрядная.
- Jatoba 5 64-разрядная.
- Tantor SE 1C 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 преднастроенных 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;
- двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
- создание резервной копии системы управления встроенными средствами системы управления;
- наличие системы контроля возникновения вирусных эпидемий;
- управления антивирусной защитой с использованием WEB консоли;
- обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;
- с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;
- использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули;
- возможность передачи ключей шифрования между серверами централизованного управления;
- выступать в качестве главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных;
- возможность экспорта и импорта выборок событий;
- возможность экспорта событий в SIEM-систему в форматах CEF или LEEF;
- возможность управления мобильными устройствами на Android и iOS;
- получение информации о программах, установленных на управляемые устройства;
- автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей и серверах под управлением Microsoft Windows;
- возможность поиска устройств по контроллерам доменов Microsoft Active Directory и Samba;
- возможность автоматизированного переноса данных с сервера администрирования под управлением ОС Windows на сервер администрирования под управлением ОС Linux;
- возможность удаленной диагностики управляемых устройств;
- поддержка кластерной технологии;
- возможность централизованного удаления несовместимого ПО с управляемых устройств;
- возможность централизованной перезагрузки управляемых устройств;
- возможность задать профили соединения для автономных пользователей с Linux-устройствами для подключения к одному и тому же или разным серверам централизованного управления в зависимости от местоположения устройства;
- поддержка контроллеров домена FreeIPA и ALD Pro;
- поддержка доменной аутентификации по Kerberos (технология единого входа, в том числе на основе сертификатов).

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

- 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:

- Потенциальный поставщик оказывает Заказчику консультационно-техническое обслуживание по вопросам настройки и эксплуатации антивирусного программного обеспечения и обеспечивает следующими возможностями:
 - Техническая поддержка должна предоставляться на русском языке специалистами производителя антивирусного ПО и его партнеров на всей территории Республики Казахстан круглосуточно в праздничные и выходные дни по телефону, электронной почте и через Интернет в течении одного года с момента продления лицензий.
 - 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.
 - Потенциальный поставщик обеспечивает доступ к электронной информационной системе технической поддержки производителя программного обеспечения, включающей в себя направление запросов по конкретным проблемам через систему электронной почты.
 - Потенциальный поставщик обеспечивает Заказчика получением технической информации и/или дополнительных программных компонентов для преодоления и разрешения проблем и ошибок, обнаруженных в программных продуктах производителя.
 - Гарантийное обслуживание и техническая поддержка программного обеспечения должно обеспечиваться без дополнительных расходов со стороны Заказчика. Гарантийное обслуживание и техническая поддержка должны осуществляться по месту нахождения программного обеспечения.
- Потенциальный Поставщик при передаче лицензии на программное обеспечение должен предоставить:**
- электронную копию письма от производителя поставляемого лицензионного программного обеспечения, подтверждающее официальные партнерские отношения с компанией-производителем, либо их официальных представителей на территории Республики Казахстан, направленное в адрес Заказчика.
 - электронные копии действующих сертификатов не менее 1-го специалиста по предлагаемому программному обеспечению.
 - в рамках продления лицензии на программное обеспечение, потенциальный Поставщик обязан провести мониторинг действующей антивирусной системы, ее обновление до актуальных версий, выполнить базовую настройку системы Заказчика.
 - потенциальный Поставщик должен провести обучение базового курса поставляемого программного продукта для одного сотрудника. По окончании обучения потенциальный Поставщик обеспечивает слушателю выдачу сертификата.

**Заместитель Председателя Правления
по финансовым и административно-
правовым вопросам**



Султанов Д.Т.

**И.О. директора департамента управления
цифровой инфраструктурой и системами**



Шаймерденова Т.К.

**Системный архитектор департамента
управления цифровой
инфраструктурой и системами**



Арыстанов Б.С.

Техникалық ерекшелік

Жұмыс станциялары мен серверлерді вирусқа қарсы қорғауға арналған қолданыстағы бағдарламалық қамтылым лицензиясының мерзімін ұзарту жөнінде.

Вирусқа қарсы қорғау (ВҚК) жұмыс станциялары мен серверлердің желіде тұрақты жұмыс істеуін қамтамасыз ететін корпоративтік шешім болуы тиіс. Ұйымның барлық бөлімшелерінде бірыңғай вирусқа қарсы құралдар пайдаланылады. Осы Техникалық ерекшелік вирусқа қарсы қорғау жүйесін енгізу бойынша ілесіп қызметтер көрсетіле отырып жеткізілетін бағдарламалық қамтылымға қойылатын талаптарды белгілейтін негізгі құжат болып табылады. Жүйенің барлық құрамдастары өзара толық біріктірілуі тиіс.

Вирусқа қарсы қорғау бағдарламалық қамтылымына қойылатын жалпы талаптар

Қолданыстағы бағдарламалық қамтылымның атауы: Kaspersky Endpoint Security for Business Advanced License — 723 лицензия.

Лицензияның қолданылу мерзімі: бағдарламалық қамтылым лицензиялары жасалған сәттен бастап кемінде 12 ай.

Жеткізу мерзімі: шарт заңды күшіне енген күннен бастап 15 күнтізбелік күннен аспайды.

Вирусқа қарсы қорғау құралдарының құрамында мыналар болуы тиіс:

- » Windows жұмыс станцияларына арналған вирусқа қарсы қорғау бағдарламалық құралдары;
- » Windows файлдық серверлеріне арналған вирусқа қарсы қорғау бағдарламалық құралдары;
- » Mac жұмыс станцияларына арналған вирусқа қарсы қорғау бағдарламалық құралдары;
- » Linux жұмыс станциялары мен серверлеріне арналған вирусқа қарсы қорғау бағдарламалық құралдары;
- » мобильді құрылғыларға (смартфондар мен планшеттерге) арналған вирусқа қарсы қорғау бағдарламалық құралдары;
- » орталықтандырылған басқару, мониторингтеу және жаңарту бағдарламалық құралдары;
- » зиянды бағдарламалар мен шабуылдар сигнатураларының жаңартылатын дерекқорлары;
- » орыс тіліндегі пайдалану құжаттамасы.

Басқару құралдарын қоса алғанда, барлық вирусқа қарсы құралдардың бағдарламалық интерфейсі орыс және ағылшын тілдерінде болуы тиіс.

Басқару құралдарын қоса алғанда, барлық вирусқа қарсы құралдардың орыс және ағылшын тілдерінде мәтінмәндік анықтамалық жүйесі болуы тиіс.

Windows жұмыс станцияларына арналған вирусқа қарсы қорғау бағдарламалық құралдарына қойылатын талаптар

Вирусқа қарсы қорғау бағдарламалық құралдары операциялық жүйелердің төменде көрсетілген нұсқалары орнатылған жұмыс станцияларында жұмыс істеуі тиіс:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 және одан жоғары;
- Windows 8 Professional / Enterprise (32 / 64 биттік);
- Windows 8.1 Professional / Enterprise (32 / 64 биттік);
- Windows 10 Home / Pro / Pro жұмыс станцияларына арналған / Education / Enterprise/Enterprise multi-session;
- Windows 11 Home / Pro / Pro жұмыс станцияларына арналған / Education / Enterprise;
- Windows 11 Arm64 үшін Home / Pro / Pro жұмыс станцияларына арналған / Education / Enterprise.

Вирусқа қарсы қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

- нақты уақыт режимінде және объектінің мәтінмәндік мәзірінен сұрау бойынша вирусқа қарсы сканерлеу;
- кесте бойынша вирусқа қарсы сканерлеу;
- қосылатын құрылғыларды вирусқа қарсы сканерлеу;
- бұрын белгісіз зиянды бағдарламаларды анықтауға және бұғаттауға мүмкіндік беретін эвристикалық талдауыш;
- белсенді жұқтыру әрекеттерін бейтараптандыру;
- зиянды белсенділікті және рұқсатсыз әрекеттерді анықтау үшін қолданбаның мінез-құлқын және жүйеде орындайтын әрекеттерін талдау;
- желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға жүгінуді талдау;
- ортақ пайдаланылатын қалталарды сырттан шифрлаудан қорғау функциясына арналған қорғау аймағын қалыптастыру;
- бағдарламалық қамтылым осалдықтарын пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, оның ішінде жүйелік процестердің жадын қорғау;
- зиянды бағдарламаны залалсыздандыру кезінде оның әрекеттерін кері қайтару, оның ішінде зиянды бағдарламалар шифрлаған файлдарды қалпына келтіру;

- процестер мен қолданбалардың артықшылықтарын шектеу (тізілімге жазу, файлдарға, калталарға, өзге процестерге және құрылғыларға қол жеткізу, тапсырмалар жоспарлағышына жүгіну, объектілерге құқықтарды өзгерту және т.б.), сенімділік деңгейі белгіленетін, динамикалық жаңартылатын қолданбалар тізімдерін баптау;
- жаңа қауіптерден бұлттық қорғау: іске қосылатын бағдарлама немесе файл жөніндегі шешімді алу үшін қолданбаның нақты уақыт режимінде өндіруші ресурстарына жүгінуі;
- RAR, ARJ, ZIP, CAB, LHA, JAR, ICE форматтарындағы архивтерде орналасқан файлдарды вирускә тексеру және емдеу;
- IMAP, SMTP, POP3, MAPI, NNTP хаттамалары арқылы берілетін кіріс және шығыс трафикті тексере отырып, электрондық поштаны зиянды бағдарламалардан қорғау;
- көрсетілген файл түрлерінің атауын өзгертуге немесе оларды жоюға мүмкіндік беретін пошта тіркемелерінің сүзгісі;
- HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP хаттамалары бойынша пайдаланушы компьютеріне келетін желілік трафикті, оның ішінде эвристикалық талдау арқылы тексеру; сенімді ресурстарды баптау және бұғаттау не статистика жинау режимдерінде жұмыс істеу мүмкіндігі;
- жүктелетін веб-беттердегі баннерлер мен қалқымалы терезелерді бұғаттау;
- фишингтік және қауіпті сайттарды анықтау және бұғаттау;
- желі сегменттерін санаттарға бөлу мүмкіндігімен желілік пакеттерге және бағдарламаларға арналған желілік ережелерді жасауға мүмкіндік беретін кірістірілген желіаралық экран;
- кез келген түрдегі есептеу желілерінде қолданбалар мен порттар үшін желіаралық экран ережелерін пайдаланып, желілік шабуылдардан қорғау;
- құрылғының MAC-мекенжайын қолдан жасау мақсатында ARP хаттамасындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;
- бірнеше желілік қосылымды бір мезгілде орнатуды бұғаттау мүмкіндігімен желілік көпір түріндегі қосылымдарды бақылау;
- барлық пайдаланушыларға немесе олардың белгілі бір топтарына (Active Directory не жергілікті пайдаланушылар/топтар) бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелерді жасау; компонент қолданбаларды бағдарлама орналасқан жол, метадеректер, сертификат немесе оның таңбасы, бақылау сомасы бойынша, сондай-ақ өндіруші алдын ала айқындаған қолданба санаттары бойынша бақылауы және қара/ақ тізім, статистика жинау немесе бұғаттау режимдерінде жұмыс істеуі тиіс;
- пайдаланушының сыртқы енгізу/шығару құрылғыларымен жұмысын құрылғы түрі және/немесе қолданылатын шина бойынша бақылау, құрылғы идентификаторлары негізінде сенімді құрылғылар тізімін жасау және Active Directory жүйесіндегі белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану құқықтарын беру;
- құрылғыларды бақылау шеңберінде барлық пайдаланушыларға немесе олардың топтарына (Active Directory не жергілікті пайдаланушылар/топтар) MTP құрылғыларын басқару және оларға қол жеткізу ережелерін баптау;
- алынбалы дискілердегі файлдардың жазылуы және/немесе жойылуы туралы оқиғаларды журналға тіркеу;
- файлдық жүйесі бар құрылғыларға қол жеткізу ережелерінің басымдығын белгілеу;
- пайдаланушының Интернеттегі жұмысын бақылау: санаттарды қосу және өңдеу, белгілі бір мазмұндағы ресурстарға және өндіруші жасайтын әрі динамикалық жаңартатын санаттарға, сондай-ақ ақпарат түрлеріне (аудио, бейне және т.б.) қол жеткізуге нақты тыйым салу немесе рұқсат беру; бақылаудың уақыт аралықтарын белгілеу және оны Active Directory жүйесінің жекелеген пайдаланушыларына тағайындау;
- BadUSB түріндегі шабуылдардан қорғау;
- қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ қолданба параметрлеріне қол жеткізуді құпиясөзбен қорғау;
- сенімді қашықтан әкімшілендіру бағдарламалары арқылы параметрлерді басқару;
- вирускә қарсы қорғау бағдарламасының тек таңдалған құрамдастарын орнату;
- жоғарыда көрсетілген барлық құрамдастарды бірыңғай басқару жүйесі арқылы орталықтандырылған басқару;
- тапсырмаларды кесте бойынша және/немесе қолданба іске қосылғаннан кейін бірден бастау;
- файлдық кеңістікті сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
- алдыңғы тексеруден кейін күйі өзгермеген объектілерді өткізіп жіберу арқылы сканерлеуді жеделдету;
- вирускә қарсы бағдарламаның тұтастығын тексеру;
- файлдың бақылау сомасы, файл/қалта атауының маскасы немесе сенімді цифрлық қолтаңбасы негізінде вирускә қарсы тексеруден алып тастау ерекшеліктерін қосу;
- ережелер мен ерекшеліктер тізімдерін XML форматында импорттау және экспорттау;
- жойылған жұқтырылған файлдарды қалпына келтіру мүмкіндігі бар қорғалған қоймада сақтау;
- антивирустың жұмыс есептеріне арналған қорғалған қойманың болуы;
- антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ мүмкіндіктер жиыны барынша азайтылған жеңілдетілген графикалық интерфейстің болуы;

- Windows Defender Security Center жүйесімен интеграция;
- Antimalware Scan Interface (AMSI) қолдауы;
- Windows Subsystem for Linux (WSL) қолдауы;
- резервтік қоймадан объектілерді қалпына келтіруді құпиясөзбен қорғау;
- Интернет қосылымы лимиттелген жағдайда желілік трафикті шектеу;
- TCP және UDP хаттамалары бойынша желіні мониторингтеу құралының болуы;
- қайта жүктеуден кейін тексеру тапсырмасын токтатылған жерінен жалғастыру;
- тапсырманы орындау ұзақтығына шектеу белгілеу;
- тексеру жүргізіліп жатқан кезде басқа тексеру тапсырмаларын кезекке қою мүмкіндігі;
- жүйені қайта жүктемей жаңарту;
- Android Debug Bridge (ADB) қолданбасында пайдаланушылардың мобильді құрылғыларға қолжетімділігін баптау;
- мобильді құрылғыға қол жеткізуге тыйым салынса да, оны USB арқылы компьютерге қосып зарядтау;
- пайдаланушылардың басып шығару құқықтарын баптау;
- Wi-Fi желілеріне қосылуды бақылау үшін WPA3 хаттамасын қолдау;
- Azure WVD жүйесімен үйлесімділік;
- iTunes қолданбасында пайдаланушылардың мобильді құрылғыларға қолжетімділігін баптау;
- компьютерде орнатылған қолданбалардың осалдықтарын анықтау және жою жөніндегі арнайы тапсырманы іске қосу, табылған осалдықтар туралы есеп беру мүмкіндігі;
- арнайы жүктеу агентін құру және Single Sign On технологиясын қолдау арқылы дискіні толық шифрлау; UEFI жүйелерін қолдау;
- жүктеу агенті немесе операциялық жүйе файлдары істен шыққанда шифрланған мазмұнды қалпына келтіру; UEFI жүйелерін қолдау;
- дискіні толық шифрлау кезінде екі факторлы аутентификацияны қолдау;
- шифрланатын мазмұнды (орналасқан жері, кеңейтімі, файлды жасаған қолданба бойынша) икемді таңдау мүмкіндігімен файлдарды шифрлау;
- таңдалған қолданбалардың шифрланған файлдарға қол жеткізуін шектеу тетіктерінің болуы, сондай-ақ ұйымнан тыс жерде файлдарды құпиясөз арқылы шифрдан шығаруға мүмкіндік беретін технологияның болуы;
- ұйым желісінен тыс жерде файлдарды шифрлауға және шифрдан шығаруға мүмкіндік беретін жұмыс режимін орнатып, алынбалы тасымалдағыштардағы деректерді шифрлау;
- бағдарламалардың мінез-құлық үлгісін қалыптастыру және осы үлгіден ауытқыған кезде олардың әрекеттерін бұғаттау (аномалияларды бейімделмелі бақылау);
- дискіні шифрлау кезінде аутентификация агентінің қызметтік есептік жазбасын жасау;
- дискіні толық шифрлау кезінде SSO жұмысы үшін ADSelfService Plus бөгде тіркелгі деректері провайдерін қолдау;
- енгізу құрылғыларын қоспағанда, барлық Bluetooth құрылғыларына қолжетімділікті шектеу және ерекшеліктерді баптау;
- операциялық жүйені қайта жүктемей қолданбаны жаңарту;
- зиянды БҚ іздеу тапсырмасы үшін процессор ресурстарын тұтынуды шектеу;
- қолданба қызметтерін сырттан басқаруға тыйым салу;
- тексеруден алып тастаудың алдын ала орнатылған ерекшеліктерін және сенімді қолданбаларды таңдау;
- жеке пайдаланушыға параметрлерді конфигурациялық файлға экспорттауға рұқсат беру;
- қолданбаға кіруге арналған уақытша құпиясөздерді бақылау және кері қайтарып алу; құпиясөздер тарихын 30 күнге дейін сақтау және мәртебесін (Белсенді, Мерзімі өткен, Кері қайтарылған) тексеру;
- Веб-бақылау ережелері тыйым салған веб-ресурстарға қосылымды саясат қолданылғаннан кейін бірден үзу;
- орнату пакетінде операциялық жүйелердің әртүрлі түрлеріне арналған құрамдастардың бөлек жинақтарын баптау;
- тексеруден алып тастаудың алдын ала орнатылған ерекшеліктерін және сенімді қолданбаларды таңдау;
- ескірген TLS 1.0 хаттамасы бойынша желілік қосылымдарды бұғаттау;
- Интернетке қол жеткізу үшін прокси-сервер арқылы қолданбаны аутентификациялау кезінде Kerberos хаттамасын қолдау;
- қолданбаны тексеруден алып тастау үшін файл хешін көрсету мүмкіндігі;

Windows серверлеріне арналған вирусқа қарсы қорғау бағдарламалық құралдарына қойылатын талаптар
 Вирусқа қарсы қорғау бағдарламалық құралдары файлдық серверлерге арналған операциялық жүйелердің төмендегі нұсқаларымен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

- Windows Small Business Server 2011 Essentials / Standard (64 биттік), Microsoft Small Business Server 2011 Standard (64 биттік) тек Microsoft Windows Server 2008 R2 үшін Service Pack 1 орнатылған жағдайда қолдау көрсетіледі;
- Windows MultiPoint Server 2011 (64 биттік);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 және одан жоғары;
- Windows Web Server 2008 R2 Service Pack 1 және одан жоғары;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (Server Core режимін қоса алғанда);
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (Server Core режимін қоса алғанда);
- Windows Server 2016 Essentials / Standard / Datacenter (Server Core режимін қоса алғанда);
- Windows Server 2019 Essentials / Standard / Datacenter (Server Core режимін қоса алғанда);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (Server Core режимін қоса алғанда).
- Windows Server 2025 Standard / Datacenter.

Вирусқа қарсы қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

- нақты уақыт режимінде және объектінің мәтінмәндік мәзірінен сұрау бойынша вирусқа қарсы сканерлеу;
- кесте бойынша вирусқа қарсы сканерлеу;
- қосылатын құрылғыларды вирусқа қарсы сканерлеу;
- бұрын белгісіз зиянды бағдарламаларды анықтауға және бұғаттауға мүмкіндік беретін эвристикалық талдауыш;
- белсенді жұқтыру әрекеттерін бейтараптандыру;
- зиянды белсенділікті және рұқсатсыз әрекеттерді анықтау үшін қолданбаның мінез-құлқын және жүйеде орындайтын әрекеттерін талдау;
- желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға жүгінуді талдау;
- бағдарламалық қамтылым осалдықтарын пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, оның ішінде жүйелік процестердің жадын қорғау;
- зиянды бағдарламаны залалсыздандыру кезінде оның әрекеттерін кері қайтару, оның ішінде зиянды бағдарламалар шифрлаған файлдарды қалпына келтіру;
- жаңа қауіптерден бұлттық қорғау: іске қосылатын бағдарлама немесе файл жөніндегі шешімді алу үшін қолданбаның нақты уақыт режимінде өндіруші ресурстарына жүгінуі;
- RAR, ARJ, ZIP, CAB, LHA, JAR, ICE форматтарындағы архивтерде орналасқан файлдарды вирусқа тексеру және емдеу;
- желі сегменттерін санаттарға бөлу мүмкіндігімен желілік пакеттерге және бағдарламаларға арналған желілік ережелерді жасауға мүмкіндік беретін кірістірілген желіаралық экран;
- құрылғының MAC-мекенжайын қолдан жасау мақсатында ARP хаттамасындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;
- қолданба қызметін қашықтан рұқсатсыз басқарудан және оның параметрлерін құпиясөз арқылы қорғау; бұл зиянды бағдарламалардың, қаскүнемдердің немесе жеткілікті білімі жоқ пайдаланушылардың қорғауды өшіруіне жол бермеуі тиіс;
- вирусқа қарсы қорғау бағдарламасының тек таңдалған құрамдастарын орнату;
- жоғарыда көрсетілген барлық құрамдастарды бірыңғай басқару жүйесі арқылы орталықтандырылған басқару;
- тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу;
- файлдық кеңістікті сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
- алдыңғы тексеруден кейін күйі өзгермеген объектілерді өткізіп жіберу арқылы сканерлеуді жеделдету;
- вирусқа қарсы бағдарламаның тұтастығын тексеру;
- файлдың бақылау сомасы, файл/қалта атауының маскасы немесе сенімді цифрлық қолтаңбасы негізінде вирусқа қарсы тексеруден алып тастау ерекшеліктерін қосу;
- жойылған жұқтырылған файлдарды қалпына келтіру мүмкіндігі бар қорғалған қоймада сақтау;
- антивирустың жұмыс есептеріне арналған қорғалған қойманың болуы;
- антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ мүмкіндіктер жиыны барынша азайтылған жеңілдетілген графикалық интерфейсін болуы;
- Windows Defender Security Center жүйесімен интеграция;
- Antimalware Scan Interface (AMSI) қолдауы;
- Windows Subsystem for Linux (WSL) қолдауы;

- резервтік қоймадан объектілерді қалпына келтіруді құпиясөзбен қорғау;
- ережелер мен ерекшеліктер тізімдерін XML форматында импорттау және экспорттау;
- Интернет қосылымы лимиттелген жағдайда желілік трафикті шектеу;
- барлық пайдаланушылар немесе белгілі бір топтар үшін (Active Directory не жергілікті пайдаланушылар/топтар) бағдарламаларды орнатуға және/немесе іске қосуға рұқсат беретін немесе тыйым салатын арнайы ережелер құру; қолданбаларды орналасқан жолы, метадеректері, сертификаты, цифрлық таңбасы, бақылау сомасы және өндіруші белгілеген санаттары арқылы бақылау; кара/ақ тізім, статистика жинау немесе бұғаттау режимдерін қолдау;
- компьютерде орнатылған қолданбалардың осалдықтарын анықтау және жою жөніндегі арнайы тапсырманы іске қосу, табылған осалдықтар туралы есеп беру мүмкіндігі;
- Windows серверлік операциялық жүйелері үшін Веб-қауіптерден қорғау, Пошталық қауіптерден қорғау, Веб-бақылау және Құрылғыларды бақылау құрамдастарын қолдау;
- қайта жүктеуден кейін тексеру тапсырмасын тоқтатылған жерінен жалғастыру;
- тапсырманы орындау ұзақтығына шектеу белгілеу;
- тексеру жүргізіліп жатқан кезде басқа тексеру тапсырмаларын кезекке қою мүмкіндігі;
- жүйені қайта жүктемей жаңарту;
- тасымалды МТР құрылғыларына қол жеткізу құқықтарын (оқу/жазу) баптау, рұқсаты бар пайдаланушыларды немесе топтарды таңдау және қол жеткізу кестесін белгілеу;
- мобильді құрылғыға қол жеткізуге тыйым салынса да, оны USB арқылы компьютерге қосып зарядтау;
- пайдаланушылардың басып шығару құқықтарын баптау;
- Wi-Fi желілеріне қосылуды бақылау үшін WPA3 хаттамасын қолдау;
- Azure WVD жүйесімен үйлесімділік;
- операциялық жүйені қайта жүктемей қолданбаны жаңарту;
- зиянды БҚ іздеу тапсырмасы үшін процессор ресурстарын тұтынуды шектеу;
- қолданба қызметтерін сырттан басқаруға тыйым салу;
- SQL серверлері, Microsoft Exchange серверлері және System Center Configuration Manager жүйесінде сенімді аймақты жылдам баптау үшін алдын ала белгіленген тексеру ерекшеліктері мен сенімді қолданбаларды пайдалану;
- Интернетке қол жеткізу үшін прокси-сервер арқылы қолданбаны аутентификациялау кезінде Kerberos хаттамасын қолдау;
- қолданбаны тексеруден алып тастау үшін файл хешін көрсету мүмкіндігі;

Мас жұмыс станцияларына арналған вирусқа қарсы қорғау бағдарламалық құралдарына қойылатын талаптар

Мас жұмыс станцияларын қорғау бағдарламалық құралдары төмендегі нұсқалардағы операциялық жүйелермен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

- macOS 12 - 15;

Вирусқа қарсы қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

- тұрақты жұмыс істейтін вирусқа қарсы мониторинг;
- жаңа қауіптерден бұлттық қорғау, яғни іске қосылатын бағдарлама немесе файл туралы қорытынды алу үшін өндірушінің арнайы ресурстарына нақты уақыт режимінде жүгіну;
- вирусқа қарсы дерекқорларды кесте бойынша автоматты жаңарту;
- жұқтырылған файлдарды қалпына келтіру мүмкіндігін сақтау үшін жою алдында олардың сақтық көшірмесін жасау;
- бұрын белгісіз зиянды бағдарламаларды анықтау және бұғаттау үшін эвристикалық талдауыш;
- желілердің, оның ішінде сымсыз желілердің барлық түрінде танымал қолданбаларға арналған желілік белсенділік ережелері мен басып кіруді анықтау және болдырмау жүйесін (IDS/IPS) пайдаланып, желілік шабуылдардан қорғау;
- өндірушінің беделді бағалау бұлттық сервистерінің қорытындылары негізінде зиянды және фишингтік сайттарды бұғаттау;
- Safari, Google Chrome және Firefox браузерлері арқылы өтетін желілік трафикті (HTTP және HTTPS) тексеру;
- Интернетке қолжетімділікті бақылау, оның ішінде санаттарды қосу және өңдеу, белгілі бір ресурстарға немесе өндіруші жасайтын және динамикалық жаңартатын ресурс санаттарына қолжетімділікке нақты рұқсат беру не тыйым салу;

- алдыңғы тексеруден кейін өзгермеген объектілерді өткізіп жіберу арқылы сканерлеуді жеделдету;
- файлдық операцияларды ұстап қалу деңгейінде көрсетілген аймақтарды тексеру үшін ерекшеліктер белгілеу;
- дискіге толық қол жеткізу құқықтарының берілуін автоматты бақылау және құқықтар берілген сәтте қажетті жүйелік кеңейтімдерді орнату;
- зиянды бағдарламаларды іздеу тапсырмалары орындалғанда колданбаның процессорға түсіретін жүктемесін шектеу;
- операциялық жүйе ресурстарына жүктемені азайту үшін бұлттық режимді қосу және зиянды бағдарламалар дерекқорының жеңілдетілген нұсқасын пайдалану;
- сұрау бойынша тексеру тапсырмаларында тек оқуға қолжетімді жүйелік томды сканерлеуді өткізіп жіберу;
- қауіпті мінез-құлық үлгілерін (BSS) пайдаланып, операциялық жүйедегі колданбалар белсенділігін талдау;
- JAMF арқылы .pkg файлынан орнату;
- сыртқы дискілер қосылған кезде оларды автоматты сканерлеу;
- клиенттік сертификаттарды қолдау;
- электрондық поштаның кіріс және шығыс хабарламалары тіркемелерін зиянды бағдарламалар мен өзге қауіптердің бар-жоғына тексеру;
- пайдаланушылардың компьютерге орнатылған немесе қосылған құрылғыларға қолжетімділігін басқару;
- Интернетте немесе жергілікті желіде жұмыс істеген кезде компьютерге рұқсатсыз қосылуларды бұғаттау және колданбалардың желілік белсенділігін бақылау;
- зиянды бағдарламаның операциялық жүйедегі файлдық, жүйелік немесе желілік әрекеттерін кері қайтару;
- эксплойттардан қорғау;
- жоғарыда аталған барлық құрамдастарды бірыңғай басқару жүйесі арқылы орталықтандырылған басқару;

Linux жұмыс станциялары мен серверлеріне арналған вирусқа қарсы қорғау бағдарламалық құралдарына қойылатын талаптар

Linux жұмыс станцияларын қорғау бағдарламалық құралдары төмендегі 32 биттік операциялық жүйелермен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12

Linux жұмыс станцияларын қорғау бағдарламалық құралдары төмендегі 64 биттік операциялық жүйелермен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

- AlmaLinux OS 8.6, 8.7, 8.8, 8.9.
- AlmaLinux OS 9.4, 9.5, 9.6.
- AlterOS® 2025.
- Amazon™ Linux 2023.
- Astra Linux Common Edition 2.12.
- Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.5).
- Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.6).
- Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.7).
- Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.8).
- Astra Linux Special Edition РУСБ.10015-03 (кезекті жаңарту 7.6).
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (кезекті жаңарту 1.6).
- Astra Linux Special Edition РУСБ.10015-17 (кезекті жаңарту 1.7.3).
- Astra Linux Special Edition РУСБ.10015-37 (кезекті жаңарту 7.7).
- CentOS 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- CentOS Stream 8.
- CentOS Stream 9.
- CentOS Stream 10.
- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12.
- Debian GNU/Linux 13.0, 13.1, 13.2.
- EMIAS 1.0.
- EulerOS 2.0 SP10.
- Fedora 41.
- Kylin 10.
- Linux Mint 21.3.
- Linux Mint 22.2.
- Mostech 12 release 2021.1.
- openSUSE Leap 15.6.
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9.
- Oracle Linux 9.4, 9.5, 9.6.

- Red Hat® Enterprise Linux® 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9.
- Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9.
- Red Hat Enterprise Linux 9.4, 9.5, 9.6.
- Red Hat Enterprise Linux 10.0, 10.1.
- Rocky Linux 8.6, 8.7, 8.8, 8.9.
- Rocky Linux 9.4, 9.5, 9.6.
- SberLinux 8.10, 9.1, 9.5, 9.6.
- SberOS 3.4.0, 3.5.0.
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7.
- SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7.
- Ubuntu® 22.04 LTS.
- Ubuntu 24.04 LTS.
- Альт Образование 10.
- Альт Образование 11.
- Альт Рабочая Станция 11.
- Альт Сервер 11.
- Альт СП Сервер шығарылым 10.
- Альт СП Рабочая Станция шығарылым 10.
- Атлант, жинақ Alcyone, нұсқа 2022.02.
- Гослинукс 7.2.
- МОС 12 Сервер release 2021.1.
- МосОС 15.5 Arbat.
- МСВСФЕРА 9.4 АРМ.
- МСВСФЕРА 9.4 СЕРВЕР.
- ОС МЭШ 12 барлық пайдаланушыларға арналған (телеметриясыз және ДИТ қолдауынсыз), release 2021.1.
- ОС МЭШ 12 Мәскеу мектептеріндегі интерактивті панельдерге арналған (телеметриямен және ДИТ қолдауымен), release 2021.1.
- ОС МЭШ 12 Мәскеу мектептеріндегі компьютерлер мен ноутбуктерге арналған (телеметриямен және ДИТ қолдауымен), release 2021.1.
- ОСнова 2.14.
- ОСнова 3.0.5.
- РЕД ОС® 7.3.
- РЕД ОС 8.0.
- РОСА "Кобальт" 7.9 Рабочая станция.
- РОСА "Кобальт" 7.9 Сервер.
- РОСА "Хром" 12 Рабочая станция.
- РОСА "Хром" 12 Сервер.
- СинтезМ-Клиент 8.6.
- СинтезМ-Сервер 8.6.

ARM архитектурасына арналған қолдау көрсетілетін 64 биттік операциялық жүйелер:

- Astra Linux Special Edition РУСБ.10152-02 (кезекті жаңарту 4.7).
- CentOS Stream 9.
- EulerOS 2.0 SP10.
- SUSE Linux Enterprise Server 15.
- Ubuntu 22.04 LTS.
- Альт СП Рабочая Станция шығарылым 10.
- Альт СП Сервер шығарылым 10.
- РЕД ОС 8.0.

Вирусқа қарсы қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

- тұрақты жұмыс істейтін вирусқа қарсы мониторинг;
- жаңа қауіптерден бұлттық қорғау: іске қосылатын бағдарлама немесе файл туралы қорытынды алу үшін қолданбаның өндірушінің арнайы ресурстарына нақты уақыт режимінде жүгінуі;
- SMB / NFS арқылы қолжетімді ресурстарды тексеру;
- ядро жадын тексеру мүмкіндігі;
- бұрын белгісіз зиянды бағдарламаларды тиімдірек анықтап, бұғаттауға мүмкіндік беретін эвристикалық талдауыш;
- пайдаланушының немесе әкімшінің пәрмені бойынша, сондай-ақ кесте бойынша вирусқа қарсы сканерлеу;
- zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj форматтарындағы архив файлдарын вирусқа тексеру;

- электрондық поштаның кіріс және шығыс хабарламаларын тексеру;
- файлдарды тексеруді оңтайландыру тетіктерінің болуы (ерекшеліктер, сенімді процестер, тексеру уақыты мен файл өлшемін шектеу, бұрын тексерілген және өзгермеген файлдар туралы ақпаратты кэштеу);
- SMB / NFS хаттамалары бойынша желілік қолжетімділігі бар жергілікті қалталардағы файлдарды қашықтан зиянды шифрлаудан қорғау;
- тексеру кезінде файлдарды бұғаттау опциясын қосу;
- күдікті және зақымдалған объектілерді карантинге орналастыру;
- SAMBA деңгейінде файлдық операцияларды ұстап қалу және тексеру;
- ережелердің бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желіаралық экранын басқару;
- тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу;
- есептерді HTML және CSV форматтарына экспорттау және сақтау;
- файлдық кеңістікті сканерлеу кезінде пайдаланушы жұмысының ыңғайлылығын қамтамасыз ету үшін компьютер ресурстарын икемді басқару;
- жұқтырылған объект ақпараттық тұрғыдан құнды болған жағдайда оны қалпына келтіру мүмкіндігі үшін емдеу және жою алдында объектінің көшірмесін резервтік қоймаға сақтау;
- goot құқықтарысыз пайдаланушының графикалық интерфейсі арқылы басқару;
- жоғарыда көрсетілген барлық құрамдастарды бірыңғай басқару жүйесі немесе веб-консоль арқылы орталықтандырылған басқару;
- құрылғы түрлері мен қосылу шиналары бойынша компьютерге орнатылған немесе қосылған құрылғыларға пайдаланушылардың қолжетімділігін басқару;
- алынбалы дискілерді тексеру;
- кіріс желілік трафикте желілік шабуылдарға тән белсенділікті бақылау;
- HTTP/HTTPS және FTP хаттамалары бойынша компьютерге түсетін трафикті тексеру және веб-мекенжайлардың зиянды немесе фишингтік ресурстарға жататынын анықтау;
- пайдаланушы компьютеріндегі бағдарламалардың әрекеттері туралы деректер алу;
- компьютерлерде сақталған бағдарламалардың барлық орындалатын файлдары туралы мәлімет алу (Түгендеу тапсырмасы);
- бағдарлама іске қосылған кезде трассалау файлдарын жасау;
- компьютерлерде орнатылған бағдарламалардың барлық орындалатын файлдары туралы мәлімет алу;
- автоматты іске қосу объектілерін, жүктеу секторларын, процестер жадын және ядро жадын тексеру;
- емдеу немесе жою алдында файлдардың сақтық көшірмелерін жасау және оларды қалпына келтіру;
- бағдарламаның жалпы параметрлерінде процестерді олардың жадын тексеруден алып тастау;
- SkipPlainTextFiles параметрі арқылы бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру;
- трафикті бағдарлама тексеруінен алып тастау;
- сұраулар мен ақпаратты шығару үшін, сондай-ақ бағдарлама және тапсырма параметрлерін экспорттау мен импорттау үшін JSON форматын пайдалану;
- Аtm архитектурасына арналған операциялық жүйелері бар құрылғыларға орнату және оларда жұмыс істеу;
- қауіп анықталғанда немесе құрылғыға қол жеткізу әрекеті тіркелгенде пайдаланушыны хабардар ету режимінде жұмыс істеу;
- тыйым салынған немесе рұқсат етілген қолданбалар тізімдері режимдерінде бақылау ережелері арқылы қорғалатын құрылғыларда қолданбаларды іске қосуды басқару;
- жаңарту кезінде қолданбаны автоматты түрде қайта іске қосу;
- процессор ресурстарын пайдалануға шектеу белгілеу;
- орнатудан кейін қолданба алғаш іске қосылғанда қорғау құрамдастары мен тексеру тапсырмаларын автоматты түрде өшіру мүмкіндігі;
- графикалық интерфейсте құрамдастар мен тапсырмалардың жұмысы туралы пайдаланушыға хабарлау;
- процестерді тоқтатпай олардың жадын оқу мүмкіндігі (Linux ядросының 3.4 нұсқасынан бастап);
- пайдаланушылардың веб-ресурстарға қолжетімділігін басқару;
- қорғалатын құрылғыларда қолданбаларды іске қосуды басқару;
- қолданбаның өз жұмысының тұрақтылығын мониторингтеу функциясы;
- тексеруден объектілерді алып тастау ерекшеліктерін баптай отырып эксплойттардан қорғау;
- қосылған құрылғылар сенімді деп есептелетін пайдаланушылар немесе пайдаланушылар топтары тізімін баптау;
- деректерді сақтау құрылғыларына тек оқу режимінде қол жеткізуге рұқсат беру;
- прокси-сервер пайдаланылғанда қолданбаның жекелеген құрамдастарына ерекшеліктер орнату;
- трафикті ұстап қалудан алып тастау ерекшеліктерін баптау;
- дерекқор журналдарының файлдарын тексеруден уақытша алып тастау;
- қолданбаға қолданылатын саясаттар мен тапсырмалардағы ерекшеліктер тізімдерін экспорттау және импорттау;

- аккумулятормен жұмыс істейтін құрылғыда жоспарланған тапсырмаларды іске қосуды болдырмауды баптау;
- пәрмен жолында қолданба функцияларының тізімін, олардың мәртебесін (пайдаланылады/пайдаланылмайды) және осы функцияларды іске асыратын Linux технологиялары туралы мәліметті шығару;
- BadUSB түріндегі шабуылдардан қорғау;
- құрылғыда қолданылатын саясат және саясат профильдері туралы ақпаратты пәрмен жолында және графикалық интерфейсте көрсету;

Мобильді құрылғыларды вирусқа қарсы қорғау бағдарламалық құралдарына қойылатын талаптар

Смартфондарды вирусқа қарсы қорғау бағдарламалық құралдары төмендегі мобильді операциялық жүйелерде жұмыс істеуі тиіс:

- Android 5.0 және одан жоғары (Android 12L қоса алғанда, Go Edition қоспағанда);
- iOS 15 және одан жоғары или iPadOS 15 және одан жоғары;

Android операциялық жүйесіндегі смартфондарға арналған вирусқа қарсы қорғау бағдарламасында мынадай функциялар іске асырылуы тиіс:

- өндірушінің бұлттық беделді бағалау сервисі арқылы қосымша тексеру деңгейін пайдалана отырып, смартфон файлдық жүйесін тұрақты вирусқа қарсы қорғау;
- құрылғының файлдық жүйесін сұрау бойынша және кесте бойынша тексеру;
- орнатылатын қолданбаларды бірден тексеру;
- өндірушінің бұлттық беделді бағалау сервисінің қорытындылары негізінде зиянды және фишингтік сайттарды бұғаттау;
- жұқтырылған объектілерді оқшаулауға арналған қойманың болуы;
- зиянды бағдарламаларды іздеуге және қауіпті объектілерді жоюға пайдаланылатын вирусқа қарсы дерекқорларды кесте бойынша жаңарту;
- көрсетілген қолданбалардың, оның ішінде алдын ала белгіленген санаттар бойынша, іске қосылуын бұғаттау;
- рұқсат етілген қолданбалардың ақ тізімдерін қолдау;
- қолданбаларды іске қосуды бақылау шеңберінде жүйелік қолданбаларды бұғаттау;
- Firebase Cloud Messaging (FCM) сервисі арқылы пәрмендер мен push-хабарламалар жіберу;
- Wi-Fi және Bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануды бұғаттау;
- Wi-Fi желілеріне қосылу параметрлерін көрсету;
- міндетті түрде орнатылуы тиіс қолданбаларды көрсету;
- мобильді құрылғыны бұғаттау, деректерді және жұмысқа қатысты деректерді жою, құрылғының орналасу координаттарын алу және зауыттық параметрлерге қашықтан қайтару (factory reset);
- корпоративтік саясаттарға сәйкестікті тексеру үшін ережелер тізімін жасау; сәйкессіздік анықталған кезде құрылғыны автоматты бұғаттау, деректерді жою және корпоративтік қолданбалардың іске қосылуына тыйым салу;
- Samsung KNOX1 және KNOX2 технологияларын қолдау;
- Android құрылғыларына арналған Қолданбаларды бақылау ережелерін жасаған кезде рұқсат етілген қолданба нұсқаларын көрсету;

Apple iOS операциялық жүйесіндегі смартфондарды қорғау құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

- топтық саясаттар арқылы iOS MDM құрылғыларының параметрлерін қашықтан баптау;
- бұғаттау және деректерді жою пәрмендерін жіберу;
- мобильді құрылғылар қауіпсіздігінің топтық саясаттарын жасау;
- Exchange ActiveSync / iOS MDM хаттамасы арқылы қосылған құрылғылардың конфигурациялық параметрлерін қашықтан баптау;
- пайдаланушылардың мобильді құрылғылары жұмысы туралы есептер мен статистиканы алу;
- supervised mode режимінде өндірушінің беделді бағалау бұлттық сервисінің қорытындылары бойынша зиянды және фишингтік сайттарды бұғаттау;
- бірыңғай басқару консолі арқылы орталықтандырылған басқару;
- басқарылатын құрылғыда iTunes, Safari немесе Game Center сияқты кірістірілген қолданбаларды пайдалануға болатынын бақылауға мүмкіндік беретін құрамдастың болуы;
- iOS MDM құрылғыларында Bluetooth параметрлерін өзгертуді тыйым салу;

Windows операциялық жүйесіне негізделген орталықтандырылған басқару, мониторингтеу және жаңарту бағдарламалық құралдарына қойылатын талаптар

Орталықтандырылған басқару, мониторингтеу және жаңарту құралдары төмендегі операциялық жүйелермен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64 биттік.

- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSC) 64 биттік.
- Windows Server 2019 Standard/Datacenter/Core 64 биттік.
- Windows Server 2022 Standard/Datacenter/Core 64 биттік.
- Windows Server 2025 Standard/Datacenter/Core 64 биттік.
- Windows Storage Server 2019 64 биттік.

Орталықтандырылған басқару, мониторингтеу және жаңарту құралдары төмендегі виртуалдандыру платформаларында орнатылуды қолдауы тиіс:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- Microsoft Hyper-V Server 2019 64 биттік.
- Microsoft Hyper-V Server 2022 64 биттік.
- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- Parallels Desktop 18.
- Oracle VM VirtualBox 7.x.

Орталықтандырылған басқару, мониторингтеу және жаңарту құралдары төмендегі нұсқалардағы дерекқорларды басқару жүйелерімен жұмыс істеуі тиіс:

- Microsoft SQL Server 2016 (барлық редакциялар) 64 биттік.
- Microsoft SQL Server 2017 (барлық редакциялар) Windows/Linux үшін 64 биттік.
- Microsoft SQL Server 2019 (барлық редакциялар) Windows/Linux үшін 64 биттік (қосымша әрекеттер қажет).
- Microsoft SQL Server 2022 (барлық редакциялар) Windows/Linux үшін 64 биттік.
- MySQL 5.7 Community 32 биттік/64 биттік.
- MySQL 8.0 Community 32 биттік/64 биттік.
- MariaDB 10.5 (жинақ 10.5.17 және одан жоғары) 32 биттік/64 биттік.
- MariaDB Galera Cluster 10.3 32 биттік/64 биттік InnoDB сақтау қосалқы жүйесімен InnoDB.
- PostgreSQL 13.x 64 биттік.
- PostgreSQL 14.x 64 биттік.
- PostgreSQL 15.x 64 биттік.
- Postgres Pro 13.x Windows/Linux 64 биттік.
- Postgres Pro 14.x Windows/Linux 64 биттік.

Вирусқа қарсы қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

- қорғалатын тораптардың санына қарай орталықтандырылған басқару, мониторингтеу және жаңарту жүйесін орнату архитектурасын таңдау;
- ұйымдағы компьютерлер мен пайдаланушылардың есептік жазбалары туралы ақпарат алу мақсатында Active Directory деректерін оқу;
- табылған компьютерлерді IP-мекенжайы, операциялық жүйе түрі және Active Directory ұйымдық бірлігінде (OU AD) орналасуы бойынша ауыстыру ережелерін баптау;
- желіде жаңа компьютерлер пайда болған кезде олардың есептік жазбаларын басқару топтарына автоматты түрде бөлу; IP-мекенжайы, ОЖ түрі және OU AD бойынша ауыстыру ережелерін баптау;
- вирусқа қарсы қорғау бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою;
- орталықтандырылған баптау және әкімшілендіру;
- қорғау құралдарының жұмысы жөніндегі есептер мен статистикалық ақпаратты қарау;
- басқару орталығы құралдарымен үйлесімсіз қолданбаларды орталықтандырылған түрде (қолмен және автоматты) жою;
- саясаттар мен тапсырмаларға енгізілген өзгерістер тарихын сақтау және алдыңғы нұсқаларға кері қайтару;
- антивирустық агенттерді орнатудың әртүрлі тәсілдері: RPC, GPO және басқару жүйесі арқылы қашықтан орнату, сондай-ақ жергілікті орнатуға арналған дербес орнату пакетін құру;
- пайдаланушының жүйеге кірген есептік жазбасына, ағымдағы IPv4-мекенжайына және компьютер орналасқан OU немесе қауіпсіздік тобына қарай вирусқа қарсы шешім параметрлерін өзгертетін арнайы триггерлерді қауіпсіздік саясаттарында белгілеу;
- қайта бөлуді айқындайтын триггерлер иерархиясы;
- жүктелген жаңартулар клиенттік компьютерлерге таратылғанға дейін оларды орталықтандырылған басқару бағдарламасы арқылы сынақтан өткізу;
- жаңартулар алынғаннан кейін оларды пайдаланушылардың жұмыс орындарына дереу жеткізу;
- бір физикалық серверде орналасқан виртуалды машиналарды желіде танып, олардың арасында іске қосылатын тапсырмалар жүктемесін теңгеру;
- әр деңгейде әкімшілер мен операторлардың құқықтарын, сондай-ақ ұсынылатын есеп нысандарын баптау мүмкіндігімен көпдеңгейлі басқару жүйесін құру;

- әкімшілендіру серверлерінің кез келген деңгейдегі иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару;
- басқару серверлері үшін көп жалдаушылық режимін (multi-tenancy) қолдау;
- байланыс арналары және машиналық ақпарат тасымалдағыштары арқылы әртүрлі дереккөздерден бағдарламалар мен вирускa қарсы дерекқорларды жаңарту;
- басқару сервері арқылы антивирус өндірушісінің бұлттық серверлеріне қол жеткізу;
- лицензияларды клиенттік компьютерлерге автоматты түрде тарату;
- пайдаланушылар компьютерлерінде орнатылған бағдарламалық қамтылым мен жабдықты түгендеу;
- орнатылған вирускa қарсы қолданбалар жұмысындағы оқиғалар туралы хабарлау механизмі және олар жөнінде электрондық пошта хабарламаларын жіберуді баптау;
- iOS MDM сервері арқылы мобильді құрылғыларды басқару функциясы;
- белгіленген оқиғалар туралы SMS-хабарламалар жіберу;
- басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату;
- басқару жүйесіне желілік жүктемені азайту үшін ұйымның кез келген компьютерін жаңартуларды қайта тарату орталығы ретінде белгілеу;
- басқару жүйесіне түсетін желілік жүктемені азайту үшін ұйымның кез келген компьютерін таңдалған клиенттер тобы агенттерінің оқиғаларын орталықтандырылған басқару серверіне жіберу орталығы ретінде белгілеу;
- вирускa қарсы қорғау оқиғалары, түгендеу деректері және орнатылған бағдарламаларды лицензиялау туралы графикалық есептер жасау;
- жүйе жұмысы бойынша алдын ала бапталған үлгілік есептердің болуы;
- есептерді PDF және XML файлдарына экспорттау;
- антивирус орнатылған желідегі барлық ресурстар бойынша резервтік қоймалар мен карантин объектілерін орталықтандырылған басқару;
- басқару серверінде аутентификациялау үшін ішкі есептік жазбаларды жасау;
- басқару жүйесінің кірістірілген құралдары арқылы оның сақтық көшірмесін жасау;
- Windows Failover Clustering қолдауы;
- Windows Certificate Authority қызметімен интеграцияны қолдау;
- пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы;
- өзін-өзі қызмет көрсету порталы пайдаланушыларға мобильді құрылғыға басқару агентін орнату, мобильді құрылғыларды қарау, бұғаттау, құрылғыны іздеу және құрылғыдағы деректерді жою пәрмендерін жіберу үшін қосылу мүмкіндігін беруі тиіс;
- вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- Microsoft Azure және Google Cloud бұлттық инфрақұрылымдарында орнату;
- OpenAPI арқылы интеграция;
- WEB-консоль арқылы вирускa қарсы қорғауды басқару;
- басқару консолі арқылы Windows операциялық жүйесін өрістетуді басқару;
- орталықтандырылған басқару құралдары пайдаланушыларының алдын ала бапталған рөлдерінің болуы;
- пайдаланушы есептік жазбаларына байланыстыру үшін нақты өкілеттіктер жиынтығы көрсетілген арнайы рөлдерді жасау мүмкіндігі;
- RDP арқылы немесе басқару консолінің штаттық құралдары арқылы қосылу;
- Windows жұмыс үстеліне бірлесіп қосылу (Windows Desktop Sharing) мүмкіндігі;
- пайдаланушыға қашықтан қосылуға рұқсат сұрауы көрсетілуі тиіс;
- ОЖ кескіндерімен жұмыс істеу құралдары: физикалық немесе виртуалды машина негізінде мақсатты ОЖ кескінін жасау және кескінді әкімші таңдаған компьютерлерге, оның ішінде операциялық жүйесі орнатылмаған компьютерлерге (bare metal) орнату;
- бұрын жасалған кескінге драйверлер жиынтықтарын қосу мүмкіндігі;
- ОЖ орнатылғаннан кейін скрипттерді іске қосу немесе қосымша БҚ-ны автоматты орнату;
- дистрибутивтерден операциялық жүйе кескінін (WIM) импорттау;
- компьютердегі үшінші тарап БҚ лицензияларын бақылау және лицензияны пайдалану шарттары бұзылғаны немесе қолданылу мерзімі аяқталғаны туралы әкімшіге хабарлау жүйесі;
- үшінші тарап қолданбаларына (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) орнату пакеттерін автоматты жасау және осы пакеттерді компьютерлерге автоматты түрде орталықтандырылған орнату;
- деректерді шифрлауды басқару функциясын қолдау;
- SIEM жүйелерімен интеграция және оқиғаларды syslog не CEF / LEEF форматтарында беру;
- Әкімшілендіру консоліне рұқсатсыз кіру тәуекелін төмендетуге арналған екі кезеңді тексеру;
- пайдаланушы есептік жазбасының параметрлері өзгергеннен кейін қосымша аутентификацияны пайдалану;
- IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылары кездесетін желілерді сұрау;
- Microsoft Windows жүйесіндегі пайдаланушы компьютерлері мен серверлердің орнатылған қолданбалары және операциялық жүйесіндегі осалдықтарды автоматты іздеу және жою;

- Әкімшілендіру серверін жоғары қолжетімді жүйе ретінде өрістетуге;
- оқшауланған желіде үшінші тарап өндірушілерінің (Microsoft бағдарламаларынан басқа) бағдарламаларын жаңарту және осалдықтарын жою;
- Windows және Linux клиенттік құрылғыларын қашықтан диагностикалау (трассалар, оқиғалар журналдары, дампытар алу, қолданбаларды тоқтату және іске қосу);
- Linux операциялық жүйесіндегі басқарылатын құрылғылардың есептік жазбаларынан жергілікті әкімші құқықтарын кері қайтарып алу;
- Linux операциялық жүйесіндегі басқарылатын құрылғылардың жергілікті есептік жазбасының құпиясөзін өзгерту;

Linux операциялық жүйесіне негізделген орталықтандырылған басқару, мониторингтеу және жаңарту бағдарламалық құралдарына қойылатын талаптар

Орталықтандырылған басқару, мониторингтеу және жаңарту құралдары төмендегі операциялық жүйелермен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

- Debian GNU/Linux 12 (Bookworm) 64 биттік.
- Debian GNU/Linux 13 (Trixie) 64 биттік.
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 биттік.
- Ubuntu Server 24.04 LTS (Noble Numbat) 64 биттік.
- CentOS Stream 9 64 биттік.
- CentOS Stream 10 64 биттік.
- Red Hat Enterprise Linux Server 7.x 64 биттік.
- Red Hat Enterprise Linux Server 8.x 64 биттік.
- Red Hat Enterprise Linux Server 9.x 64 биттік.
- Red Hat Enterprise Linux Server 10.x 64 биттік.
- SUSE Linux Enterprise Server 12 (барлық жаңарту пакеттері) 64 биттік.
- SUSE Linux Enterprise Server 15 (барлық жаңарту пакеттері) 64 биттік.
- Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.6) 64 биттік.
- Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.7) 64 биттік.
- Astra Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.8) 64 биттік.
- Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (кезекті жаңарту 1.6) 64 биттік.
- Astra Linux Special Edition РУСБ.10015-17 (кезекті жаңарту 1.7.3) 64 биттік.
- Astra Linux Special Edition RUSB.10015-03 (кезекті жаңарту 7.6) 64 биттік.
- Astra Linux Special Edition РУСБ.10015-37 (кезекті жаңарту 7.7) 64 биттік.
- Astra Linux Common Edition (кезекті жаңарту 2.12) 64 биттік.
- Альт СП Сервер 10 64 биттік.
- Альт СП Рабочая станция 10 64 биттік.
- Oracle Linux 7 64 биттік.
- Oracle Linux 8 64 биттік.
- Oracle Linux 9 64 биттік.
- Platform V SberLinux OS Server (SLO) 8.10.1 64 биттік.
- Platform V SberLinux OS Server (SLO) 9.5.1 64 биттік.
- Platform V SberLinux OS Server (SLO) 9.6 64 биттік.
- РЕД ОС 7.3 Сервер 64 биттік.
- РЕД ОС 7.3 Сертификатталған редакция 64 биттік.
- РЕД ОС 8 64 биттік.
- РОСА "КОБАЛЬТ" 7.9 64 биттік.
- М ОС (Moscow Electronic School) 12 Сервер 64 биттік.
- Mostech Server 64 биттік.
- MocOS 15.5 Arbat 64 биттік.

Орталықтандырылған басқару, мониторингтеу және жаңарту құралдары төмендегі виртуалдандыру платформаларына орнатылуды қолдауы тиіс:

- VMware vSphere 6.7.0.
- VMware vSphere 7.0.3.
- Microsoft Hyper-V Server 2019 64 биттік.
- Microsoft Hyper-V Server 2022 64 биттік.
- Citrix XenServer 7.x.
- Citrix XenServer 8.2.
- Parallels Desktop 18.
- Oracle VM VirtualBox 7.0.12.
- Kernel-based Virtual Machine (барлық қолдау көрсетілетін Linux ОЖ).

Орталықтандырылған басқару, мониторингтеу және жаңарту құралдары төмендегі дерекқорларды басқару жүйелерінің нұсқаларымен жұмыс істеуі тиіс:

- MySQL 5.7 Community 32 биттік/64 биттік.
- MySQL Standard Edition 8.0 (шығарылым 8.0.20 және одан жоғары) 32 биттік/64 биттік.
- MySQL Enterprise Edition 8.0 (шығарылым 8.0.20 және одан жоғары) 32 биттік/64 биттік.
- MySQL Standard Edition 8.4 32 биттік/64 биттік.
- MySQL Enterprise Edition 8.4 32 биттік/64 биттік.
- MariaDB 10.1 (жинақ 10.1.30 және одан жоғары) 32 биттік/64 биттік.
- MariaDB 10.3 (жинақ 10.3.22 және одан жоғары) 32 биттік/64 биттік.
- MariaDB 10.4 (жинақ 10.4.20 және одан жоғары) 32 биттік/64 биттік.
- MariaDB 10.5 (жинақ 10.5.27 және одан жоғары) 32 биттік/64 биттік.
- MariaDB 10.6 (жинақ 10.6.20 және одан жоғары) 32 биттік/64 биттік.
- MariaDB 10.11 (жинақ 10.11.10 және одан жоғары) 32 биттік/64 биттік.
- MariaDB Galera Cluster 10.3 32 биттік/64 биттік InnoDB сақтау қосалқы жүйесімен InnoDB.
- PostgreSQL 13.x 64 биттік.
- PostgreSQL 14.x 64 биттік.
- PostgreSQL 15.x 64 биттік.
- PostgreSQL 15.x 64 биттік (кластер Corosync/Pacemaker).
- PostgreSQL 16.x 64 биттік.
- PostgreSQL 17 64 биттік.
- PostgreSQL 18 64 биттік.
- Postgres Pro 13.x (барлық редакциялар) 64 биттік.
- Postgres Pro 14.x (барлық редакциялар) 64 биттік.
- Postgres Pro 15.x (барлық редакциялар) 64 биттік.
- Postgres Pro 15.x 64 биттік (кластер Corosync/Pacemaker).
- Postgres Pro 16.x (барлық редакциялар) 64 биттік.
- Postgres Pro 16.x Enterprise 64 биттік (кластер Built-in High Availability).
- Postgres Pro 17 (барлық редакциялар) 64 биттік.
- Postgres Pro 17 Enterprise 64 биттік (кластер Built-in High Availability).
- Postgres Pro 18 (барлық редакциялар) 64 биттік.
- Postgres Pro 18 Enterprise 64 биттік (кластер Built-in High Availability).
- Platform V Pangolin 6.5.1 64 биттік.
- Platform V Pangolin 6.5.1 64 биттік (кластер Built-in High Availability).
- Jatoba 4 64 биттік.
- Jatoba 5 64 биттік.
- Tantor SE 1C 64 биттік.

Вирусқа қарсы қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

- вирусқа қарсы қорғау құралдарын орталықтандырылған орнату, жаңарту және жою;
- орталықтандырылған баптау және әкімшілендіру;
- қорғау құралдарының жұмысы туралы есептер мен статистикалық ақпаратты қарау;
- саясаттар мен тапсырмаларды өзгерту тарихын сақтау және алдыңғы нұсқаларға кері қайтару;
- қайта бөлуді айқындайтын триггерлер иерархиясы;
- жаңартуларды алынғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу;
- бір физикалық серверде орналасқан виртуалды машиналарды анықтау және олардың арасындағы іске қосылатын тапсырмалардың жүктемесін теңгеру;
- әр деңгейде әкімшілер мен операторлардың құқықтарын және есеп беру нысандарын баптай отырып, көпдеңгейлі басқару жүйесін құру;
- әкімшілендіру серверлерінің кез келген деңгейдегі иерархиясын жасау және бүкіл иерархияны жоғары деңгейден орталықтандырылған басқару;
- басқару серверлері үшін көп жалдаушылық режимін (multi-tenancy) қолдау;
- бағдарламалар мен вирусқа қарсы дерекқорларды байланыс арналары немесе ақпарат тасымалдағыштары арқылы әртүрлі көздерден жаңарту;
- басқару сервері арқылы өндірушінің бұлттық серверлеріне қол жеткізу;
- лицензияларды клиенттік компьютерлерге автоматты тарату;
- орнатылған антивирустық қолданбалардың жұмысы туралы оқиғалар жөнінде хабарлау және электрондық пошта хабарламаларын жіберуді баптау тетігі;
- вирусқа қарсы қорғау оқиғалары мен бағдарламаларды лицензиялау деректері бойынша графикалық есептер құрастыру;
- жүйе жұмысы туралы алдын ала бапталған үлгілік есептердің болуы;
- есептерді PDF және XML форматтарына экспорттау;

- антивирус орнатылған барлық желілік ресурстардағы резервтік қоймалар мен карантин объектілерін орталықтандырылған басқару;
- басқару серверінде аутентификацияға арналған ішкі есептік жазбаларды жасау;
- Әкімшілендіру консоліне рұқсатсыз қол жеткізу тәуекелін азайту үшін екі кезеңді тексеру;
- басқару жүйесінің кірістірілген құралдарымен сақтық көшірме жасау;
- вирустық эпидемиялардың туындауын бақылау жүйесінің болуы;
- WEB-консоль арқылы вирусқа қарсы қорғауды басқару;
- әкімшілендіру серверіне түсетін жүктемені азайту және корпоративтік желі трафигін оңтайландыру үшін басқарылатын құрылғыларға вирусқа қарсы дерекқорлар мен бағдарламалық модульдерді әкімшілендіру сервері арқылы да, тарату нүктелері арқылы да жаңарту және тарату;
- жаңартуларды басқарылатын құрылғыларға орнатпас бұрын олардың жұмысқа жарамдылығын және қателерін тексеруге арналған жаңартуларды тексеру тапсырмасын пайдалану;
- вирусқа қарсы дерекқорлар мен бағдарламалық модульдерді жүктеу үшін айырмашылық файлдары функциясын пайдалану;
- орталықтандырылған басқару серверлері арасында шифрлау кілттерін беру;
- негізгі сервер ретінде жұмыс істеу және Linux немесе Windows операциялық жүйелеріндегі бағынышты серверлерді басқару;
- оқиғалар іріктемелерін экспорттау және импорттау;
- оқиғаларды SIEM жүйесіне CEF немесе LEEF форматтарында экспорттау;
- Android және iOS мобильді құрылғыларын басқару;
- басқарылатын құрылғыларға орнатылған бағдарламалар туралы мәлімет алу;
- Microsoft Windows жүйесіндегі пайдаланушы компьютерлері мен серверлерінде орнатылған қолданбалар мен операциялық жүйенің осалдықтарын автоматтандырылған түрде іздеу және жою;
- Microsoft Active Directory және Samba домен контроллерлері бойынша құрылғыларды іздеу;
- Windows операциялық жүйесіндегі әкімшілендіру серверінен Linux операциялық жүйесіндегі әкімшілендіру серверіне деректерді автоматтандырылған көшіру;
- басқарылатын құрылғыларды қашықтан диагностикалау;
- кластерлік технологияны қолдау;
- басқарылатын құрылғылардан үйлесімсіз бағдарламалық қамтылымды орталықтандырылған жою;
- басқарылатын құрылғыларды орталықтандырылған қайта жүктеу;
- Linux құрылғылары бар автономды пайдаланушыларға құрылғының орналасуына қарай бір немесе әртүрлі орталықтандырылған басқару серверлеріне қосылу үшін қосылым профильдерін белгілеу;
- FreeIPA және ALD Pro домен контроллерлерін қолдау;
- Kerberos бойынша домендік аутентификацияны (оның ішінде сертификаттарға негізделген бірыңғай кіру технологиясын) қолдау;

Вирусқа қарсы дерекқорларды жаңартуға қойылатын талаптар

Жаңартылатын вирусқа қарсы дерекқорлар мынадай функционалдық мүмкіндіктерді қамтамасыз етуі тиіс:

- бір күнтізбелік тәулік ішінде вирусқа қарсы дерекқорларды кемінде 24 рет жаңарту ережелерін жасау;
- жаңартудың бірнеше тәсілінің болуы, оның ішінде байланыс арналары және алынбалы электрондық ақпарат тасымалдағыштары арқылы;
- электрондық цифрлық қолтаңба құралдарымен жаңартулардың тұтастығы мен түпнұсқалығын тексеру;

Пайдалану құжаттамасына қойылатын талаптар

- вирусқа қарсы қорғау құралдарымен бірге берілетін құжаттамада тиісті құралды орнату, баптау және пайдалану процесі егжей-тегжейлі сипатталуы тиіс;

Техникалық қолдауға қойылатын талаптар

Вирусқа қарсы бағдарламалық қамтылымның техникалық қолдауы төмендегі талаптарға сай болуы тиіс:

Әлеуетті өнім беруші Тапсырыс берушіге вирусқа қарсы бағдарламалық қамтылымды баптау және пайдалану мәселелері бойынша консультациялық-техникалық қызмет көрсетеді және мынадай мүмкіндіктерді қамтамасыз етеді: Техникалық қолдауды вирусқа қарсы БҚ өндірушісінің және оның серіктестерінің мамандары Қазақстан Республикасының бүкіл аумағында орыс тілінде, мереке және демалыс күндерін қоса алғанда, тәулік бойы телефон, электрондық пошта және Интернет арқылы лицензияларды ұзартқан сәттен бастап бір жыл бойы көрсетуі тиіс.

Вирусқа қарсы шешім өндірушісінің веб-сайты орыс тілінде болуы, вирусқа қарсы шешімді техникалық қолдауға арналған арнайы бөлімі, толықтырылып отыратын білім базасы және бағдарламалық өнімдер пайдаланушыларының форумы болуы тиіс.

Әлеуетті өнім беруші бағдарламалық қамтылым өндірушісінің нақты мәселелер бойынша электрондық пошта жүйесі арқылы сұраулар жіберуге мүмкіндік беретін электрондық техникалық қолдау ақпараттық жүйесіне қолжетімділікті қамтамасыз етеді.

Әлеуетті өнім беруші Тапсырыс берушіге өндірушінің бағдарламалық өнімдерінде анықталған мәселелер мен қателерді жою үшін техникалық ақпаратты және/немесе қосымша бағдарламалық құрамдастарды алуды қамтамасыз етеді.

Бағдарламалық қамтылымға кепілдік қызмет көрсету мен техникалық қолдау Тапсырыс беруші үшін қосымша шығынсыз қамтамасыз етілуі тиіс. Кепілдік қызмет көрсету және техникалық қолдау бағдарламалық қамтылым орналасқан жерде көрсетілуі тиіс.

Бағдарламалық қамтылым лицензиясын берген кезде әлеуетті өнім беруші мыналарды ұсынуы тиіс:

жеткізілетін лицензиялық бағдарламалық қамтылым өндірушісінен немесе оның Қазақстан Республикасындағы ресми өкілдерінен Тапсырыс берушінің атына жолданған, өндірушімен ресми серіктестік қатынастарды растайтын хаттың электрондық көшірмесі;

ұсынылатын бағдарламалық қамтылым бойынша кемінде бір маманның қолданыстағы сертификаттарының электрондық көшірмелері;

бағдарламалық қамтылым лицензиясын ұзарту шеңберінде әлеуетті өнім беруші қолданыстағы вирусқа қарсы жүйеге мониторинг жүргізуге, оны өзекті нұсқаларға жаңартуға және Тапсырыс беруші жүйесінің базалық баптауын орындауға міндетті;

әлеуетті өнім беруші бір қызметкерге жеткізілетін бағдарламалық өнім бойынша базалық оқу курсын өткізуі тиіс. Оқу аяқталғаннан кейін әлеуетті өнім беруші тыңдаушыға сертификат берілуін қамтамасыз етеді.

**Басқарма Төрағасының қаржы
және әкімшілік-құқықтық
мәселелер жөніндегі орынбасары**



Султанов Д.Т.

**Цифрлық инфрақұрылым және
жүйелерді басқару департаментінің
директорының м.а.**



Шаймерденова Т.Қ.

**Цифрлық инфрақұрылым және
жүйелерді басқару департаментінің
жүйелік архитекторы**



Арыстанов Б.С.