Утверждаю

\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ ФИО

# ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Предмет закупки:

Передача права на использование

Kaspersky Total Security for Business 5000+Node 1 year Renewal License

для АКБ «Микрокредитбанк»

Ташкент

2025

Оглавление

[ТЕХНИЧЕСКОЕ ЗАДАНИЕ 1](#_Toc200473601)

[Наименование и спецификация предмета закупки 3](#_Toc200473602)

[Общие требования к поставщику 3](#_Toc200473603)

[Требования к обновлению антивирусных баз 3](#_Toc200473604)

[Требования к эксплуатационной документации 3](#_Toc200473605)

[Требования к технической поддержке 3](#_Toc200473606)

[Общие технические требования 4](#_Toc200473607)

[Требования к программным средствам антивирусной защиты для рабочих станций Windows 4](#_Toc200473608)

[Требования к программным средствам антивирусной защиты для серверов Windows 7](#_Toc200473609)

[Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux 9](#_Toc200473610)

[Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows 12](#_Toc200473611)

[Требования к системе защиты веб-трафика 15](#_Toc200473612)

[Требования к программным средствам антивирусной защиты и фильтрации спама с помощью отдельного сервера 18](#_Toc200473613)

[Требования к программным средствам антивирусной защиты и фильтрации спама для почтовых серверов, установленных на операционную систему семейства Linux 20](#_Toc200473614)

[Требования к программным средствам антивирусной защиты и фильтрации спама для серверов Microsoft Exchange 23](#_Toc200473615)

[Требования к программным средствам централизованного управления, мониторинга и обновления 25](#_Toc200473616)

# Наименование и спецификация предмета закупки

|  |  |  |  |
| --- | --- | --- | --- |
| Артикул | Наименование | Номер лицензии | Количество |
| KL48692AYFR | Передача права на использование Kaspersky Total Security for Business 5000+Node 1 year Renewal License | 2946-240628-101701-646-2471 | 4600 |

# Общие требования к поставщику

* Опыт аналогичных поставок не менее 3 лет.
* Наличие действующего партнерского сертификата не ниже уровня «Silver».
* Не менее двух сертифицированных инженеров, наличие сертификатов обязательно.

# Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

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

# Требования к эксплуатационной документации

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

* «Руководство пользователя (администратора)»

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

# Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

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

# Общие технические требования

Антивирусные средства должны включать:

* программные средства антивирусной защиты для рабочих станций Windows;
* программные средства антивирусной защиты для рабочих станций и серверов Linux;
* программные средства антивирусной защиты для файловых серверов Windows;
* программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows.
* программные средства антивирусной защиты веб-трафика;
* программные средства антивирусной защиты и фильтрации спама с помощью отдельного сервера
* программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux;
* программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange;
* 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 SP1 (32 / 64-разрядная);
* 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 (TH1, TH2, RS1, RS2,RS3, RS4, RS5, 19H1, 19H2, 20H1, 20H2, 21H1, 21H2, 22H2) (с ограничениями);
* Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise (версии 22H2, 23H2) (с ограничениями).

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

* поддержку определенных ролей и их ассоциации с конкретными администраторами безопасности, администраторами серверов или пользователями;
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности;
* получение и установку обновлений в автоматизированном режиме, в том числе с сетевого ресурса;
* получение и установку обновлений без применения средств автоматизации;
* генерацию записи аудита для событий, подвергаемых аудиту;
* чтение информации из записей аудита;
* ассоциацию событий аудита с идентификаторами субъектов;
* ограничение доступа к чтению записей аудита;
* поиск, сортировку, упорядочение данных аудита;
* выполнение проверок с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;
* выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
* выполнение проверок с целью обнаружения зараженных объектов по команде;
* выполнение проверок с целью обнаружения зараженных объектов в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
* выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* удаление (если удаление технически возможно) вредоносного кода из оперативной памяти, удаления файлов, в которых обнаружен вредоносный код, а также файлов, с подозрением на наличие вредоносного кода;
* возможность перемещения и изолирования зараженных объектов, удаления вредоносного кода из файлов и системных областей носителей информации;
* возможность блокирования АРМ, на котором обнаружены зараженные файлы;
* возможность восстановления функциональных свойств зараженных объектов;
* отображение сигнала тревоги об обнаружении вредоносных объектов;
* возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью
* возможность контроля доступа к веб-ресурсам
* возможность контроля за запуском ПО на защищаемом АРМ.
* антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
* фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
* проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
* блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
* распознавания и блокировку фишинговых и небезопасных сайтов;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
* возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* возможность управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
* записи в журнал событий о записи и/или удалении файлов на съемных дисках;
* контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
* защиты от атак типа BadUSB;
* запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуск задач по расписанию и/или сразу после запуска приложения;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* возможность проверки целостности антивирусной программы;
* возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* возможность включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
* возможность интеграции с Windows Defender Security Center;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* возможность защитить паролем восстановление объектов из резервного хранилища.
* 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).

# 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);
* Windows MultiPoint Server 2011 (64-разрядная);
* Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная);
* Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная);
* Windows Server 2012 Foundation / Essentials / Standard (64-разрядная);
* Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная);
* Windows Server 2016 (64-разрядная) (с ограничениями);
* Windows Server 2019 (64-разрядная) (с ограничениями)
* Windows Server 2022 (64-разрядная) (с ограничениями).

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

* поддержку определенных ролей и их ассоциации с конкретными администраторами безопасности и администраторами серверов;
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности;
* получение и установку обновлений в автоматизированном режиме, в том числе с сетевого ресурса;
* получение и установку обновлений без применения средств автоматизации;
* генерацию записи аудита для событий, подвергаемых аудиту;
* чтение информации из записей аудита;
* ассоциацию событий аудита с идентификаторами субъектов;
* ограничение доступа к чтению записей аудита;
* поиск, сортировку, упорядочение данных аудита;
* выполнение проверок с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;
* выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
* выполнение проверок с целью обнаружения зараженных объектов по команде;
* выполнение проверок с целью обнаружения зараженных объектов в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
* выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* удаление (если удаление технически возможно) вредоносного кода из оперативной памяти, удаления файлов, в которых обнаружен вредоносный код, а также файлов, с подозрением на наличие вредоносного кода;
* возможность перемещения и изолирования зараженных объектов, удаления вредоносного кода из файлов и системных областей носителей информации;
* возможность блокирования АРМ, на котором обнаружены зараженные файлы;
* возможность восстановления функциональных свойств зараженных объектов;
* отображение сигнала тревоги об обнаружении вредоносных объектов;
* возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью
* возможность контроля за запуском ПО на защищаемом сервере.
* антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
* облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* возможность проверки целостности антивирусной программы;
* возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* возможность включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
* возможность интеграции с Windows Defender Security Center;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* возможность защитить паролем восстановление объектов из резервного хранилища.

# Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux

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

* CentOS 6.10;
* Debian GNU/Linux 11.8;
* Debian GNU/Linux 12.2;
* Red Hat Enterprise Linux 6.10;
* Альт 8 СП Рабочая Станция;
* Альт 8 СП Сервер;
* Альт Рабочая Станция релиз 10;
* Альт СП Рабочая Станция релиз 10

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

* AlmaLinux OS 8.8;
* AlmaLinux OS 9.2;
* AlterOS 7.5;
* Amazon Linux 2;
* Astra Linux Common Edition (обновление 2.12);
* Astra Linux Special Edition 5;
* CentOS 6.10;
* CentOS 7.9;
* CentOS Stream 8;
* CentOS Stream 9;
* Debian GNU/Linux 11.8;
* Debian GNU/Linux 12.2;
* EMIAS 1.0;
* EulerOS 2.0 SP5;
* Kylin 10;
* Linux Mint 20.3;
* Linux Mint 21.2;
* openSUSE Leap 15.5;
* Oracle Linux 7.10;
* Oracle Linux 8.8;
* Oracle Linux 9.2;
* Red Hat Enterprise Linux 6.10;
* Red Hat Enterprise Linux 7.9;
* Red Hat Enterprise Linux 8.8;
* Red Hat Enterprise Linux 9.2;
* Rocky Linux 8.8;
* Rocky Linux 9.2;
* SberLinux 8.8 (Dykhtau);
* SUSE Linux Enterprise Server 12 SP5;
* SUSE Linux Enterprise Server 15 SP5;
* Ubuntu 20.04 LTS;
* Ubuntu 22.04 LTS;
* Альт 8 СП Рабочая станция;
* Альт 8 СП Сервер;
* Альт СП Рабочая Станция релиз 10;
* Альт СП Сервер релиз 10;
* Альт Рабочая Станция релиз 10;
* Альт Сервер релиз 10;
* Атлант, сборка Alcyone, версия 2022.02;
* Гослинукс 7.17;
* Гослинукс 7.2;
* МСВСФЕРА 9.2 СЕРВЕР;
* МСВСФЕРА 9.2 АРМ;
* РЕД ОС 7.3;
* РЕД ОС 8;
* РОСА "Кобальт" 7.9;
* РОСА "Хром" 12;
* СинтезМ-Клиент 8.6;
* СинтезМ-Сервер 8.6.

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

* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности;
* получение и установку обновлений в автоматизированном режиме, в том числе с сетевого ресурса;
* получение и установку обновлений без применения средств автоматизации;
* генерацию записи аудита для событий, подвергаемых аудиту;
* чтение информации из записей аудита;
* ассоциацию событий аудита с идентификаторами субъектов;
* ограничение доступа к чтению записей аудита;
* поиск, сортировку, упорядочение данных аудита;
* выполнение проверок с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации;
* выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
* выполнение проверок с целью обнаружения зараженных объектов по команде;
* выполнение проверок с целью обнаружения зараженных объектов в режиме динамического обнаружения в процессе выполнения операций доступа к объектам;
* выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* удаление (если удаление технически возможно) вредоносного кода из оперативной памяти, удаления файлов, в которых обнаружен вредоносный код, а также файлов, с подозрением на наличие вредоносного кода;
* возможность перемещения и изолирования зараженных объектов, удаления вредоносного кода из файлов и системных областей носителей информации;
* возможность блокирования АРМ и серверов, на которых обнаружены зараженные файлы;
* возможность восстановления функциональных свойств зараженных объектов;
* отображение сигнала тревоги об обнаружении вредоносных объектов.
* резидентного антивирусного мониторинга;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* проверку ресурсов доступных по SMB / NFS;
* эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
* проверку сообщений электронной почты в текстовом формате (Plain text);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* возможность включения опции блокирования файлов во время проверки;
* помещение подозрительных и поврежденных объектов на карантин;
* проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов;
* возможность перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
* возможность управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
* 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;
* проверки памяти ядра.

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

Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

32-разрядных операционных систем Microsoft Windows

* Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Server 2008 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше.

64-разрядных операционных систем Microsoft Windows

* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Microsoft Small Business Server 2008 Standard / Premium;
* Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;
* Microsoft Small Business Server 2011 Essentials / Standard;
* Microsoft Windows MultiPoint™ Server 2011 Standard / Premium;
* Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
* Microsoft Windows MultiPoint Server 2012 Standard / Premium;
* Windows Storage Server 2012;
* Windows Hyper-V Server 2012;
* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
* Windows Storage Server 2012 R2;
* Windows Hyper-V Server 2012 R2;
* Windows Server 2016 Essentials / Standard / Datacenter;
* Windows Server 2016 MultiPoint;
* Windows Server 2016 Core Standard / Datacenter;
* Microsoft Windows MultiPoint Server 2016;
* Windows Storage Server 2016;
* Windows Hyper-V Server 2016;
* Windows Server 2019 Essentials / Standard / Datacenter;
* Windows Server 2019 Core;
* Windows Storage Server 2019;
* Windows Hyper-V Server 2019.
* Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15.

Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

* возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
* возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
* возможность читать информацию из записей аудита;
* ограничение доступа к чтению записей аудита;
* поиск, сортировка и упорядочение данных аудита;
* возможность уполномоченным пользователям управлять данными (административными данными), используемыми функциями безопасности;
* возможность уполномоченным пользователям управлять режимом выполнения функций безопасности;
* возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
* возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
* возможность удаления (если технически возможно) файлов, в которых обнаружен вредоносный код, а также файлов, подозрительных на наличие вредоносного кода, перемещение и изолирование объектов воздействия;
* возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы;
* возможность отображение сигнала тревоги об обнаружении на рабочей станции администратора, в том числе до подтверждения его получения или до завершения сеанса;
* возможность восстановления функциональных свойств зараженных объектов;
* возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения;
* возможность выполнять проверки с целью обнаружения атаки эксплойтов в памяти процессов, в контейнерах Windows Server 2016 и Windows Server 2019;
* возможность при обнаружении признаков атаки эксплойтов на защищаемый процесс завершать процесс, сообщать о факте дискредитации уязвимости в процессе;
* возможность проведения проверки целостности компонентов программного изделия.
* антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
* защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
* непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
* анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* возможность проверки контейнеров Microsoft Windows;
* защиты от эксплуатирования уязвимостей в памяти процессов;
* должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
* возможность добавлять процессы в список защищаемых;
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
* настройки проверки критических областей сервера в качестве отдельной задачи;
* регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;
* возможность продолжать антивирусное сканирование в фоновом режиме;
* наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
* ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
* возможность интеграции с SIEM системами;
* возможность указания количества рабочих процессов антивируса вручную;
* возможность отключить графический интерфейс;
* наличие удаленной и локальной консоли управления;
* управления параметрами антивируса из командной строки;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил.
* защита от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
* защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления;
* наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп);
* компонент создания специальных правил должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
* компонент создания специальных правил должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должен иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
* осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем;
* информирование администратора о подключении внешних устройств;
* наличие механизмов автоматической генерации правил для контроля устройств и приложений.

# Требования к системе защиты веб-трафика

Система должна поставляться в виде

* RPM- или DEB- пакета, содержащего дистрибутив программы для защиты и контроля трафика
* RPM- пакета, содержащего дистрибутив программы для защиты и контроля трафика, а также для управления прокси-сервером squid (appliance-исполнение)

Система должна поддерживать установку и работу на следующих 64-битных операционных системах:

* Red Hat Enterprise Linux® 7.7, 8;
* Ubuntu 18.04.3 LTS;
* Debian 9.11, 10.1;
* SUSE Linux® Enterprise Server 15 SP1;
* CentOS 7.7;
* Astra Linux Special Edition 1.6;
* ALT Linux 8.

Система в appliance-исполнении должна поддерживать работу на операционной системе CentOS 7.7

Система должна поддерживать установку на физический и виртуальный сервер, для работы в виртуальной среде должна поддерживать установку на следующие гипервизоры:

* VMware ESXi 6.5 Update 2 / 6.7 Update 1.
* Microsoft Hyper-V Server 2016 / 2019.

Программные средства должны обеспечивать следующие возможности:

* поддержка определенных ролей для системы защиты веб-трафика и их ассоциации с конкретными администраторами безопасности и администраторами серверов или корпоративными пользователями
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности системы защиты веб-трафика
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности системы защиты веб-трафика
* получение и установка обновлений без применения средств автоматизации и в автоматизированном режиме с сетевого ресурса
* генерация записей аудита для событий, подвергаемых аудиту
* чтение информации из записей аудита
* ассоциация событий аудита с идентификаторами субъектов
* ограничение доступа к чтению записей аудита
* поиск, сортировку, упорядочение данных аудита
* выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени
* выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* удаление (если удаление технически возможно) вредоносного кода
* блокирование доступа к зараженным файлам
* предоставление возможности блокирования сервера, на котором обнаружены зараженные файлы
* отображение сигнала тревоги об обнаружении вредоносного объекта
* выполнение фильтрации сообщений протокола ICAP
* выполнение аутентификации и идентификации администраторов системы
* обнаруживать и лечить вирусы в любых типах файлов и вложений.
* блокировать вредоносные и фишинговые веб-сайты.
* использовать дополнительный уровень проверки на основе репутационных облачных сервисов производителя антивирусных средств защиты для обеспечения более высокой скорости реакции на угрозы, не дожидаясь обновления баз программы, а также снижения вероятности ложных срабатываний.
* осуществлять контроль и защиту SSL-шифрованного сетевого трафика при замене сертификата на стороне прокси-сервера.
* поддерживать интеграцию с прокси-сервером по протоколу ICAP
* настраивать правила доступа и защиты на основании следующих критериев:
  + Категория веб-сайта
  + URL ресурса
  + Имя файла
  + Тип файла
  + Размер файла
  + MIME-тип
  + Хеш-сумма файла
  + Направление трафика
  + HTTP-метод
  + LDAP-запись
  + User-agent
  + IP-адрес или маска подсети
* настраивать приоритет выполнения прав доступа и защиты
* выполнять контроль доступа пользователей к Интернет-ресурсам на основании категорий веб-сайтов и типов контента, определенных производителем средства защиты.
* поддержка в качестве фильтра URL-адресов масок и регулярных выражений.
* осуществлять контроль использования пользователями только определенного типа веб-обозревателя (блокирование запрещенных в управляемых организациях браузер-клиентов).
* осуществлять настройку временного расписания правил контроля доступа пользователей к Интернет-ресурсам.
* интегрироваться с Microsoft Active Directory для назначения ролей пользователям управляющей консоли.
* обеспечивать возможность интеграции с несколькими доменами Microsoft Active Directory.
* обеспечивать поддержку NTLM- и Kerberos-аутентификации для службы единого входа (Single Sign-On).
* осуществлять поддержку рабочих областей для выделенных групп на основании сетевых адресов, масок подсетей, LDAP-записей.
* настраивать индивидуальные правила обработки и проверки трафика для рабочих областей.
* настраивать вид веб-страницы, информирующей пользователя о блокировке Интернет-ресурса.
* вести статистику работы, включающую в себя помимо прочего информацию о выполнении и результатах антивирусной проверки, ошибках в работе приложения и предупреждениях.
* позволять экспортировать журналы событий программы в формат CSV.
* расследовать инциденты доступа в интернет с помощью поиска и просмотра событий.
* карточка события помимо прочего должна включать в себя:
  + URL
  + протокол
  + домен
  + результат детектирования технологиями защиты
  + время наступления события
  + имя пользователя
  + User Agent пользователя
  + IP-адрес пользователя
* публиковать события программы в систему корреляции событий (SIEM) по протоколу Syslog. При этом информация о каждом событии должна передаваться как отдельное syslog-сообщение в формате CEF.
* обеспечивать возможность сбора диагностической информации о программе через веб-интерфейс
* настраивать параметры программы и управлять программой через веб-интерфейс
* поддерживать возможность импортировать и экспортировать значения параметров программы
* получать статистику работы программы по протоколу SNMP, включать и отключать отправку SNMP-ловушек
* осуществлять мониторинг состояния работы программы, сетевого трафика, обрабатываемого программой, количества проверенных и обнаруженных объектов, последних и наиболее часто встречающихся угроз, заблокированных пользователей и URL-адресов через web-интерфейс программы
* обновлять антивирусные базы, как с сайта компании – производителя (по защищенному и незащищенному http-протоколу), так и из настраиваемых ресурсов (HTTP- и FTP-серверов) по расписанию или по требованию.
* настраивать параметры прокси-сервера через веб-интерфейс программы (при развертывании appliance-исполнения)
* возможность группировать созданные правила доступа и защиты
* создавать правила обхода для веб-ресурсов, не требующих обработки механизмами защиты и контроля доступа
* возможность задать правила защиты по умолчанию
* возможности управления встроенным прокси-сервером через веб интерфейс программы
* подключение доверенных балансировщиков нагрузки к встроенному прокси серверу с поддержкой заголовков PROXY protocol и HTTP Forwarded
* аутентификация пользователей на встроенном прокси сервере с использованием Kerberos и NTLM
* возможность осуществлять дешифрацию HTTPS трафика на встроенном прокси сервере c использованием самоподписанного или корпоративного сертификата
* возможность создавать правила дешифрации трафика на встроенном прокси сервере, в том числе для исключения ресурсов по IP и доменным именам из правил дешифрации
* возможность добавления отпечатков доверенных сертификатов в хранилище системы
* возможность управления форматом хранения журнала работы прокси-сервера
* возможность кластеризации решения
* возможность централизованного управления и мониторинга серверов системы, собранных в кластер
* должна поддерживаться возможность интеграции с системами типа «песочница» для оправки файлов, полученных системой защиты веб-трафика для анализа, а также для получения результатов сканирования
* возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF

# Требования к программным средствам антивирусной защиты и фильтрации спама с помощью отдельного сервера

Система должна поддерживать установку на физический и виртуальный сервер, для работы в виртуальной среде должна поддерживать установку на следующие гипервизоры:

* VMware ESXi 6.5 Update 3.
* VMware ESXi 6.7 Update 3b.
* VMware ESXi 7.0 Update 2d.
* Microsoft Hyper-V Server 2016 (только Generation 1).
* Microsoft Hyper-V Server 2019.
* KVM, запущенный на QEMU 2.12 на базе CentOS 7.

Программные средства должны обеспечивать следующие возможности:

* поддержка определенных ролей для системы защиты веб-трафика и их ассоциации с конкретными администраторами безопасности и администраторами серверов или корпоративными пользователями
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности системы защиты
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности системы защиты
* получение и установка обновлений без применения средств автоматизации и в автоматизированном режиме с сетевого ресурса
* генерация записей аудита для событий, подвергаемых аудиту
* чтение информации из записей аудита
* ассоциация событий аудита с идентификаторами субъектов
* ограничение доступа к чтению записей аудита
* поиск, сортировку, упорядочение данных аудита
* выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени
* выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* удаление (если удаление технически возможно) вредоносного кода
* выполнение проверок сообщений электронной почты на предмет наличия незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)
* поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
* проверка входящего потока почтовых сообщений на наличие спама, потенциального спама, массовых рассылок (в том числе маркетинговых рассылок), удаление выявленных сообщений, помещение копии сообщений в карантин;
* наличие общего карантина сообщений;
* управление карантином из веб-интерфейса;
* детектирование вредоносных и фишинговых ссылок в теле письма;
* наличие эвристических методов детектирования;
* возможность использования репутационных облачных сервисов;
* возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
* наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;
* обнаруживать, блокировать и лечить зараженные почтовые сообщения и зараженные вложения, удалять сообщения и вложения, помещать копии сообщений в карантин;
* обнаруживать и блокировать сообщения, содержащие макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять сообщения или вложения, помещать копии сообщений в карантин;
* обнаруживать и блокировать сообщения, содержащие зашифрованные объекты, удалять сообщения или вложения, помещать копии сообщений в карантин;
* обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов, блокировать отдельные файлы внутри архивов;
* выполнять контентную фильтрацию сообщений по имени, размеру и типу вложений, определять формат и тип вложения, независимо от его расширения, удалять сообщения, содержащие вложения определенного формата или с определенным именем или сообщения, размер которых превышает допустимый, помещать копии сообщений в хранилище;
* сохранять резервные копии сообщений в карантине по результатам их обработки модулями защиты;
* сохранять сообщения из карантина в файл и пересылать сообщения получателям;
* возможность развертывания кластерной архитектуры почтовых серверов с возможностью централизованного управления для масштабирования решения (как горизонтально, так и вертикально);
* интеграции со службами каталогов Active Directory и Open LDAP;
* возможность отправки ловушек по протоколу SNMP;
* обрабатывать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей;
* отправлять уведомления пользователям о результатах проверки их сообщений модулями программы;
* поддерживать работу персонального карантина на основе LDAP-записей;
* доступ к персональному карантину должен осуществляться на основе учетных записей LDAP;
* отправлять уведомления пользователям о состоянии персонального карантина, уведомления должны содержать список последних сообщений в карантине;
* настройки расписания отправки уведомлений;
* обновлять базы программы с серверов обновлений "Лаборатории Касперского" и пользовательских ресурсов (HTTP- и FTP-серверов) по расписанию и по требованию;
* отправлять и получать сообщения по защищенному каналу TLS/SSL, осуществлять управление ключами шифрования;
* осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC;
* подписывать исходящие сообщения электронной почты с помощью технологии DKIM;
* добавлять предупреждения о небезопасном вложении к входящим сообщениям в теме письма;
* просматривать журнал событий, аудита в веб интерфейсе программы и загружать его на жесткий диск;
* централизованное управление карантином сообщений всех почтовых серверов в кластерном исполнении;
* фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
* проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
* проверка с помощью сервиса SPAM URI Realtime Blocklists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
* проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
* выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка;
* перенос в карантин зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы, а также файлы, в результате проверки которых произошла ошибка;
* использование регулярных выражений при создании правил фильтрации;
* в правилах фильтрации сообщений электронной почты указывать пользователей и группы пользователей из Microsoft Active Directory и generic LDAP;
* наличие встроенных ролей администратора и специалиста поддержки;
* возможность уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем заражённые и подозрительные объекты;
* управление работой программы должно осуществлять как стандартными средствами операционной системы с помощью командной строки, так и через специальный веб-интерфейс, работающий на браузерах: Internet Explorer, Mozilla Firefox, Google Chrome;
* наличие ролевой модели разграничения доступа пользователей к функциям программы;
* возможность помечать сообщения специальной меткой, при обнаружении уязвимости Bussiness Email Compromise Detection (BEC);
* должна поддерживаться возможность интеграции с системами типа «песочница» для отправки файлов, полученных системой защиты веб-трафика для анализа, а также для получения результатов сканирования;
* возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF;
* обнаруживать сообщения с Юникод-спуфингом. В случае обнаружения Юникод-спуфинга считаеть сообщение спамом.
* возможность управления маршрутизацией почтового трафика через веб-интерфейс;
* настраивать режимы TLS-шифрования сообщений для ситуаций, когда система принимает сообщения от другого сервера (действует как Сервер) или пересылает сообщения на другой сервер (действует как Клиент), а также настраивать параметры TLS для отдельных доменов.

# Требования к программным средствам антивирусной защиты и фильтрации спама для почтовых серверов, установленных на операционную систему семейства Linux

Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать на компьютерах, имеющих следующие минимальные конфигурации вычислительной среды:

* ОС СН «Astra Linux Special Edition» (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* PostgreSQL 9, PostgreSQL 11 (из состава ОС СН «Astra Linux Special Edition»);
* Exim 4;
* Apache HTTP Server 2.4.46 и выше

Программные средства должны обеспечивать следующие возможности:

* поддержка определенных ролей для системы защиты веб-трафика и их ассоциации с конкретными администраторами безопасности и администраторами серверов или корпоративными пользователями
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности системы защиты
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности системы защиты
* получение и установка обновлений без применения средств автоматизации и в автоматизированном режиме с сетевого ресурса
* генерация записей аудита для событий, подвергаемых аудиту
* чтение информации из записей аудита
* ассоциация событий аудита с идентификаторами субъектов
* ограничение доступа к чтению записей аудита
* поиск, сортировку, упорядочение данных аудита
* выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени
* выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* удаление (если удаление технически возможно) вредоносного кода
* информирование об обнаружении вредоносного кода
* поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
* проверка входящего потока почтовых сообщений на наличие спама, потенциального спама, массовых рассылок (в том числе маркетинговых рассылок), удаление выявленных сообщений, помещение копии сообщений в карантин;
* наличие общего карантина сообщений;
* управление карантином из веб-интерфейса;
* детектирование вредоносных и фишинговых ссылок в теле письма;
* наличие эвристических методов детектирования;
* возможность использования репутационных облачных сервисов;
* возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
* наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;
* обнаруживать, блокировать и лечить зараженные почтовые сообщения и зараженные вложения, удалять сообщения и вложения, помещать копии сообщений в карантин;
* обнаруживать и блокировать сообщения, содержащие макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять сообщения или вложения, помещать копии сообщений в карантин;
* обнаруживать и блокировать сообщения, содержащие зашифрованные объекты, удалять сообщения или вложения, помещать копии сообщений в карантин;
* обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов, блокировать отдельные файлы внутри архивов;
* выполнять контентную фильтрацию сообщений по имени, размеру и типу вложений, определять формат и тип вложения, независимо от его расширения, удалять сообщения, содержащие вложения определенного формата или с определенным именем или сообщения, размер которых превышает допустимый, помещать копии сообщений в хранилище;
* сохранять резервные копии сообщений в карантине по результатам их обработки модулями защиты;
* сохранять сообщения из карантина в файл и пересылать сообщения получателям;
* интеграции со службами каталогов Active Directory и Open LDAP;
* возможность отправки ловушек по протоколу SNMP;
* обрабатывать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей;
* отправлять уведомления пользователям о результатах проверки их сообщений модулями программы;
* поддерживать работу персонального карантина на основе LDAP-записей;
* доступ к персональному карантину должен осуществляться на основе учетных записей LDAP;
* отправлять уведомления пользователям о состоянии персонального карантина, уведомления должны содержать список последних сообщений в карантине;
* настройки расписания отправки уведомлений;
* обновлять базы программы с серверов обновлений "Лаборатории Касперского" и пользовательских ресурсов (HTTP- и FTP-серверов) по расписанию и по требованию;
* отправлять и получать сообщения по защищенному каналу TLS/SSL, осуществлять управление ключами шифрования;
* осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC;
* добавлять предупреждения о небезопасном вложении к входящим сообщениям в теме письма;
* просматривать журнал событий, аудита в веб интерфейсе программы;
* фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
* проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
* проверка с помощью сервиса SPAM URI Realtime Blocklists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
* проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
* выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка;
* перенос в карантин зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы, а также файлы, в результате проверки которых произошла ошибка;
* использование регулярных выражений при создании правил фильтрации;
* в правилах фильтрации сообщений электронной почты указывать пользователей и группы пользователей из Microsoft Active Directory и generic LDAP;
* наличие встроенных ролей администратора и специалиста поддержки;
* возможность уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем заражённые и подозрительные объекты;
* управление работой программы должно осуществлять как стандартными средствами операционной системы с помощью командной строки, так и через специальный веб-интерфейс, работающий на браузерах: Internet Explorer, Mozilla Firefox, Google Chrome;
* возможность помечать сообщения специальной меткой, при обнаружении уязвимости Bussiness Email Compromise Detection (BEC).
* должна поддерживаться возможность интеграции с системами типа «песочница» для оправки файлов, полученных системой защиты веб-трафика для анализа, а также для получения результатов сканирования
* возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF;
* обнаруживать сообщения с Юникод-спуфингом. В случае обнаружения Юникод-спуфинга считать сообщение спамом.

# Требования к программным средствам антивирусной защиты и фильтрации спама для серверов Microsoft Exchange

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

* Microsoft Windows Server 2019 Standard или Datacenter (Desktop Experience);
* Microsoft Windows Server 2019 Core;
* Microsoft Windows Server 2016 Standard или Datacenter;
* Microsoft Windows Server® 2012 R2 Standard или Datacenter.

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать с программным обеспечением Microsoft Exchange Server следующих версий:

* Microsoft Exchange Server 2019, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
* Microsoft Exchange Server 2016, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
* Microsoft Exchange Server 2013 SP1, развернутый как минимум в одной из следующих ролей: Почтовый ящик, Пограничный транспорт или Сервер клиентского доступа (CAS).

Консоль управления программными средствами антивирусной защиты для серверов Microsoft Exchange должна быть реализована с использованием Microsoft Management Console и должна функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

* Microsoft Windows Server 2019 Standard или Datacenter (Desktop Experience);
* Microsoft Windows Server 2019 Core;
* Microsoft Windows Server 2016 Standard или Datacenter;
* Microsoft Windows Server 2012 R2 Standard или Datacenter;
* Microsoft Windows 10;
* Microsoft Windows 8.1;
* Microsoft Windows 8.

Программные средства должны обеспечивать следующие возможности:

* поддержка определенных ролей для системы защиты веб-трафика и их ассоциации с конкретными администраторами безопасности и администраторами серверов или корпоративными пользователями
* возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности системы защиты
* возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности системы защиты
* получение и установка обновлений без применения средств автоматизации и в автоматизированном режиме с сетевого ресурса
* генерация записей аудита для событий, подвергаемых аудиту
* чтение информации из записей аудита
* ассоциация событий аудита с идентификаторами субъектов
* ограничение доступа к чтению записей аудита
* поиск, сортировку, упорядочение данных аудита
* выполнение проверок с целью обнаружения зараженных объектов в режиме реального времени
* выполнение проверок с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
* удаление (если удаление технически возможно) вредоносного кода
* информирование об обнаружении вредоносного кода
* управление входящими информационными потоками для выявления и удаления спама
* совместимость с DAG в Microsoft Exchange;
* поиск и удаление по требованию всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
* поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в хранящихся на сервере Microsoft Exchange (в том числе в общих папках) сообщениях, включая вложения;
* проверка почтовых хранилищ и общих папок на сервере, в фоновом режиме для гарантированной обработки всех объектов с использованием самой актуальной версии антивирусных баз без заметного увеличения нагрузки на сервер;
* возможность лечить зараженные архивы;
* возможность выявления и удаления не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы, программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях;
* возможность детектирования вредоносных и фишинговых ссылок в теле письма;
* сохранение копий изменяемых сообщений в резервном хранилище, что позволяет восстановить важную информацию в случае некорректного лечения объекта;
* набор параметров поиска для удобства нахождения объекта в резервном хранилище;
* дополнительный уровень проверки с помощью репутационных облачных сервисов;
* возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
* наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;
* проверка различных параметров письма, таких как адреса отправителей и получателей, размер письма, а также поля заголовка сообщения;
* фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
* проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
* проверка IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF);
* проверка с помощью сервиса SPAM URI Realtime Block lists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
* использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и файлов вложений);
* возможность использовать роли пользователей/администраторов для разграничения доступа к настройкам безопасности;
* аудит изменения параметров программы по событиям в журнале событий Windows;
* мониторинг состояния программы, получение статистики работы программы и управление белыми и черными списками адресов Анти-Спама с помощью команд в среде Windows PowerShell;
* использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и имён файлов);
* возможность фильтрации файлов Microsoft Office, содержащих макросы;
* возможность проверки и удаления сообщений, являющихся спамом или содержащих фишинговые и вредоносные ссылки;
* проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
* создание отчетов по работе системы защиты;
* возможность автоматической рассылки отчетов администраторам по расписанию;
* возможность обновления антивирусных баз как с сайтов производителя, так и с внутренних сетевых ресурсов организации;
* возможность фоновой проверки почтовых ящиков и общих папок с использованием Exchange Web Services;
* детальные отчеты в формате HTML;
* наличие возможности отправки отчётов и уведомлений на указанные адреса электронной почты;
* мониторинг работы программы с помощью System Center - Operations Manager;
* интеграция с Active Directory;
* централизованный просмотр состояния защиты.

# Требования к программным средствам централизованного управления, мониторинга и обновления

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

* Windows Server 2008 R2 Standard Service Pack 2 или более поздняя версия 64-разрядная;
* Windows Server 2008 R2 Service Pack 2 (все редакции) 64-разрядная;
* Windows Server 2012 Server Core 64-разрядная; • Windows Server 2012 Datacenter 64-разрядная;
* Windows Server 2012 Essentials 64-разрядная;
* Windows Server 2012 Foundation 64-разрядная;
* Windows Server 2012 Standard 64-разрядная;
* Windows Server 2012 R2 Server Core 64-разрядная;
* Windows Server 2012 R2 Datacenter 64-разрядная;
* Windows Server 2012 R2 Essentials 64-разрядная;
* Windows Server 2012 R2 Foundation 64-разрядная;
* Windows Server 2012 R2 Standard 64-разрядная;
* Windows Server 2016 Datacenter (LTSB) 64-разрядная;
* Windows Server 2016 Standard (LTSB) 64-разрядная;
* Windows Server 2016 (вариант установки Server Core) (LTSB) 64- разрядная;
* Windows Server 2019 Standard 64-разрядная;
* Windows Server 2019 Datacenter 64-разрядная;
* Windows Server 2019 Core 64-разрядная;
* Windows Server 2022 Standard 64-разрядная;
* Windows Server 2022 Datacenter 64-разрядная;
* Windows Server 2022 Core 64-разрядная;
* Windows Storage Server 2012 64-разрядная;
* Windows Storage Server 2012 R2 64-разрядная;
* Windows Storage Server 2016 64-разрядная;
* Windows Storage Server 2019 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления, под управлением операционных систем Windows, должны функционировать с СУБД следующих версий:

* Microsoft SQL Server 2012 Express 64-разрядная;
* Microsoft SQL Server 2014 Express 64-разрядная;
* Microsoft SQL Server 2016 Express 64-разрядная;
* Microsoft SQL Server 2017 Express 64-разрядная;
* Microsoft SQL Server 2019 Express 64-разрядная;
* Microsoft SQL Server 2014 (все редакции) 64-разрядная;
* Microsoft SQL Server 2016 (все редакции) 64-разрядная;
* Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;
* Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная;
* Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная;
* Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная;
* Microsoft Azure SQL Database;
* Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;
* 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;
* 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 10.4.26 и выше) 32-разрядная/64-разрядная;
* MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная;
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
* MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
* PostgreSQL 13.x 64-разрядная;
* PostgreSQL 14.x 64-разрядная;
* Postgres Pro Standard 13.x 64-разрядная;
* Postgres Pro Standard 14.x 64-разрядная;
* Postgres Pro Certified 14.x 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления, под управлением операционных систем Windows, должны поддерживать установку на следующих виртуальных платформах:

* VMware vSphere 6.7;
* VMware vSphere 7.0;
* VMware Workstation 16 Pro;
* Microsoft Hyper-V Server 2012 64-разрядная;
* Microsoft Hyper-V Server 2012 R2 64-разрядная;
* Microsoft Hyper-V Server 2016 64-разрядная;
* Microsoft Hyper-V Server 2019 64-разрядная;
* Microsoft Hyper-V Server 2022 64-разрядная;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x.
* Parallels Desktop 17
* Oracle VM VirtualBox 6.x (только гостевой вход Windows)

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

* Debian GNU/Linux 10.х (Buster) 64-разрядная.
* Debian GNU/Linux 11.х (Bullseye) 64-разрядная.
* Debian GNU/Linux 12 (Bookworm) 64-разрядная.
* Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная.
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная.
* Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
* CentOS 7.x 64-разрядная.
* CentOS Stream 9 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.
* SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная.
* SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
* Astra Linux Special Edition3 РУСБ.10015-01 64-разрядная.
* Astra Linux Common Edition (обновление 2.12) 64-разрядная.
* Альт СП Сервер 10 64-разрядная.
* Альт Сервер 10 64-разрядная.
* Альт Сервер 9.2 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная.
* Oracle Linux 7 64-разрядная.
* Oracle Linux 8 64-разрядная.
* Oracle Linux 9 64-разрядная.
* РЕД ОС 7.3 Сервер 64-разрядная.
* РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
* РОСА "КОБАЛЬТ" 7.9 64-разрядная

Программные средства централизованного управления, мониторинга и обновления, под управлением операционных систем Linux, должны функционировать с СУБД следующих версий:

* MySQL 5.7 Community 32-разрядная/64-разрядная.
* MySQL 8.0 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 10.4.26 и выше) 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.х 64-разрядная.
* PostgreSQL 14.х 64-разрядная.
* PostgreSQL 15.х 64-разрядная.
* Postgres Pro 13.х (все редакции) 64-разрядная.
* Postgres Pro 14.х (все редакции) 64-разрядная.
* Postgres Pro 15.х (все редакции) 64-разрядная.
* Platform V Pangolin 5.4.0 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления, под управлением операционных систем Linux, должны поддерживать установку на следующих виртуальных платформах:

* VMware vSphere 6.7.
* VMware vSphere 7.0.
* VMware vSphere 8.0.
* VMware Workstation 16 Pro.
* VMware Workstation 17 Pro.
* Microsoft Hyper-V Server 2012 64-разрядная.
* Microsoft Hyper-V Server 2012 R2 64-разрядная.
* Microsoft Hyper-V Server 2016 64-разрядная.
* Microsoft Hyper-V Server 2019 64-разрядная.
* Microsoft Hyper-V Server 2022 64-разрядная.
* Citrix XenServer 7.1 LTSR.
* Citrix XenServer 8.x.
* Parallels Desktop 17.
* Oracle VM VirtualBox 6.x.
* Oracle VM VirtualBox 7.x
* Виртуальная машина на основе Kernel (все операционные системы Linux, поддерживаемые Сервером администрирования.

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

* генерация записи аудита для событий, подвергаемых аудиту;
* чтение информации из записей аудита;
* ассоциация событий аудита с идентификаторами субъекта;
* ограничение доступа к чтению записей аудита;
* поиск, сортировка данных аудита;
* обработка зараженных объектов на АРМ и серверах вычислительной сети;
* выполнение автоматизированного запуска на АРМ и серверах вычислительной сети с заданными условиями поиска вредоносных объектов и режимами реагирования по расписанию;
* выполнение удаленного администрирования процессов обнаружения вредоносных объектов, обновления базы данных признаков вредоносных компьютерных программ (БД ПКВ) и компонентов;
* возможность уполномоченным пользователям управлять параметрами настройки функций безопасности;
* возможность создания учетных записей и идентификации/аутентификации пользователей;
* отображение сигнала тревоги на автоматизированном рабочем месте администратора безопасности, указывающего на обнаружение вредоносных объектов на пользовательских автоматизированных рабочих местах.
* выполнение получения и установки обновлений БД ПКВ без применения средств автоматизации и в автоматизированном режиме в том числе с сетевого ресурса;
* выполнение централизованной установки компонентов.
* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* возможность настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
* автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по IPv4-адресу, типу ОС, нахождению в OU AD;
* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
* возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* возможность иерархии триггеров, по которым происходит перераспределение;
* тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* инвентаризация установленного ПО и оборудования на компьютерах пользователей;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* функция управления мобильными устройствами через сервер Exchange ActiveSync (только для Windows);
* функция управления мобильными устройствами через сервер iOS MDM (только для Windows);
* возможность отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства (только для Windows);
* возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
* построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* поддержка Windows Failover Clustering;
* поддержка интеграции с Windows сервисом Certificate Authority (только для Windows);
* наличие веб-консоли управления приложением;
* наличие системы контроля возникновения вирусных эпидемий (только для Windows);
* возможность установки в облачной инфраструктуре Microsoft Azure и Google Cloud (только для Windows);
* возможность интеграции по OpenAPI ;
* возможность управления антивирусной защитой с использованием WEB консоли.
* автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей (только для Windows);
* возможность подключения по RDP или штатными средствами из консоли управления, пользователю должен выводиться запрос на разрешение дистанционного подключения (только для Windows);
* наличие инструментов работы с образами ОС: cоздание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры (только для Windows);
* должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;
* возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС (только для Windows);
* возможность импортировать образ операционной системы из дистрибутивов (WIM) (только для Windows);
* наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии (только для Windows);
* автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры (только для Windows);
* поддержка функциональности управления шифрованием данных (только для Windows);
* возможность интеграции с SIEM системами.