ОРИЁНБОНК

Информационное сообщение

Нткоытйа Хкцийнаонйа йбщартвй «Ноихнбйнк» поиглХшХат йогХнизХции поинять счХртиа в йтбйоа (йткоытйм кйнксора) нХ пйртХвкс гйдйвйе лицанзии пойгоХммнйгй йбарпачания Kaspersky Endpoint Security for Business Advanced для НЎН «Ноихнбйнк» (НднХ тырячХ лицанзие). НогХнизХции, пойшадшае йтбйо и поадлйжившае нХибйлаа поиамламыа срлйвия рйтосдничартвХ,поадйртХвляатряпоХвй зХключания дйгйвйоХ нХ пйртХвксгйдйвйе лицанзии пойгоХммнйгй йбарпачания Kaspersky Endpoint Security for Business Advanced для НЎН «Ноихнбйнк». Изващаниа и кйнксорнХя дйксмантХция поилХгХютря к нХртйящамс рййбщанию.

Хасан Асадуллозода
Председатель

Тел.: (37) 221-05-68; Факс: (37) 221-18-77
info@oriyonbonk.tj, www.oriyonbonk.tj

ОРИЁНБОНК

Извещение

О проведении открытого конкурса на поставку годовой лицензии программного обеспечения Kaspersky Endpoint Security for Business Advanced для ОАО «Ориёнбонк»

Основные сведения о проведении конкурса:

1. **форма торгов:** открытый конкурс;
2. **заказчик: наименование:** Открытое акционерное общество «Ориёнбонк»;
   - **почтовый адрес:** Республика Таджикистан, 734001, г. Душанбе, пр. Рудаки 95/1
   - **место нахождения:** Республика Таджикистан, г. Душанбе пр. Рудаки 95/1
   - **адрес электронной почты:** **l.sharipova@oriyonbonk.tj**
   - **номер контактного телефона заказчика:** +992 (37) 221 08 21;
3. **источник финансирования заказа:** собственные средства заказчика
4. **предмет конкурса:** выбор компаний на поставку годовой лицензии программного обеспечения Kaspersky Endpoint Security for Business Advanced для ОАО «Ориёнбонк».
5. **порядок и сроки проведения конкурса:**

   – К участию в Конкурсе приглашаются организации (далее - «Участники Конкурса»), зарегистрированные на территории Республики Таджикистан, имеющие опыт работы по предмету Конкурса и отвечающие требованиям Конкурсной документации:
   – Официальный сайт, на котором размещена конкурсная документация: **www.oriyonbonk.tj** в разделе «Тендеры»:
   – Размер, порядок и сроки внесения платы, взимаемой заказчиком, за предоставление конкурсной документации, если такая плата установлена: плата за предоставление конкурсной документации заказчиком не установлена.
   - **количество победителей Конкурса** – один или несколько**.**
   - **дата объявления Конкурса** – 04 октября .2024г.
   - **дата подачи материалов** - не позднее 16^{00} часов – 14 октября 2024г.
   - **дата вскрытия конвертов** - не позднее – 14 октября 2024г.

   Материалы на Конкурс предоставляются в **запечатанных конвертах** (опечатанных печатью Участника Конкурса) с указанием наименования подающих их компаний и наименования Конкурса.

   Вся документация Конкурсной заявки может быть продублирована в электронном виде на CD/DVD диске (текстовые файлы - в формате *.rtf, таблицы - *.xlsx, остальные документы — в формате *.pdf или *.MPP) и вложена в запечатанный конверт с материалами, отправляемыми на Конкурс.

   Конверты адресуются на имя секретаря Тендерной комиссии, **Шариповой Лилии Давлатовной** с пометкой: **"Конкурс на годовой лицензии программного обеспечения Kaspersky Endpoint Security for Business Advanced для ОАО «Ориёнбонк»**

   Адрес Конкурсного комитета: 734001, г. Душанбе, пр. Рудаки, 95/1.
   Материалы, направленные в конвертах, оформленных ненадлежащим образом или полученные после указанного срока, рассматриваться не будут.
   Дополнительную информацию по вопросам проведения Конкурса можно получить: **Шарипова Лилия Давлатовна**, e-mail: **l.sharipova@oriyonbonk.tj**, номер тел. **+992 (37) 221 08 21**
6. **Квалификационные требования к Участникам Конкурса**

   К участию в Конкурсе допускаются компании или частные предприниматели с и без образования юридического лица, удовлетворяющие перечисленным ниже критериям;
   – Опыт работы организации-претендента в сфере поставки программного обеспечения не менее 3 лет;
   – Не приостановление деятельности участника размещения заказа в порядке, предусмотренном Кодексом Республики Таджикистан об административных правонарушениях, на день рассмотрения заявки на участие в конкурсе;
   – Не проведение процедуры ликвидации или банкротства компании претендента;

– Устойчивое финансовое положение компании - претендента;
– Документы или копии документов, подтверждающих соответствие участника размещения заказа установленным требованиям и условиям допуска к участию в конкурсе:
– Отзывы от крупных организаций (желательно) и другие существенные документы, характеризующие Участника Конкурса.

7. **Требования к предмету конкурса**

– техническое задание представлено во вложении;
– Согласно требованиям, указанным в (**Приложении №2**).

8. **Документы, предоставляемые Участниками Конкурса**

– Конкурсная заявка по форме **Приложения № 1**;
– Копия свидетельства о государственной регистрации;
– Предложение по стоимости поставляемых услуг, выполненное в произвольном формате, с указанием цены;
– Копия свидетельства о государственной регистрации;
– Копии лицензий на осуществление деятельности, являющейся предметом Конкурса;
– Копия свидетельства о постановке на налоговый учет и справка из налогового органа об отсутствии задолженности по **уплате налогов**;
– Копии документов, подтверждающих полномочия должностных лиц на совершение сделок, являющихся предметом конкурса (решение уполномоченных органов об избрании руководителя);
– Копии сертификатов, определяющих статус партнерства с крупными компаниями и копии других документов, подтверждающих авторизацию Участника Конкурса от фирм-производителей;
– Отзывы от крупных организаций (желательно) и другие существенные документы, характеризующие Участника Конкурса.

9. **Валюта Конкурсной заявки**

– Все стоимостные показатели документов, входящих в состав Конкурсной документации, должны быть выражены **в сомони с учетом НДС;**
– Выражение денежных сумм в другой валюте считается существенным отклонением от требований и условий настоящей Конкурсной документации и может привести к отклонению Конкурсной заявки.

10. **Затраты на участие в Конкурсе**

Участник Конкурса несет все расходы, связанные с подготовкой и подачей своей заявки, а Организатор Конкурса не отвечает и не имеет обязательств по этим расходам, независимо от характера проведения и результатов Конкурса.

11. **Цены коммерческих предложений**

– На предмет Конкурсной заявки должны быть указаны специальные цены для ОАО «Ориёнбонк»;
– Цены, предлагаемые Участниками Конкурса, должны включать НДС и другие возможные затраты, и обязательные платежи (**страхование, уплата налогов, таможенные пошлины, сборы**);
– Цены, предлагаемые Участниками Конкурса, должны быть фиксированными на момент заключения договора.

12. **Оформление и подписание заявки**

– Все документы, представленные на Конкурс, включая копии и прайс-листы, должны быть сшиты в единую книгу, пронумерованы и скреплены печатью компании и подписью уполномоченного лица или лиц, подписывающих заявку;
– Никакие исправления не будут иметь силу, за исключением тех случаев, когда они подписаны лицом или лицами, подписывающими заявку.

Извещение

13. **Изменения в заявках**

- Участник Конкурса вправе изменить (прислать новую) или отозвать свою заявку до истечения срока представления заявок. Уведомление об изменении заявки или об её отзыве должно быть направлено Организатору до истечения срока представления заявок;
- Никакие изменения в заявки не вносятся после истечения срока их подачи.

14. **Вскрытие Конкурсным комитетом конвертов с заявками**

- Вскрытие конвертов с заявками будет производиться членами Конкурсного комитета в сроки, указанные в **п. 5.**

15. **Критерии оценки Конкурсных заявок**

- Оценка и сопоставление коммерческих предложений, и определение победителей конкурса производится по наиболее оптимальному соотношению всех критериев оценки и сопоставления коммерческих предложений:
  a) Соответствие Участника Конкурса квалификационным требованиям;
  b) Соответствие предоставленного материала требованиям к документам Участника Конкурса;
  c) Стоимость поставляемых услуг.

16. **Разъяснение Конкурсных заявок**

- Во время рассмотрения Конкурсных заявок Организатор Конкурса может, по своему усмотрению, попросить Участника Конкурса дать разъяснения по поводу информации, содержащейся в его заявке или запросить от Участника недостающие документы. При этом не должно поступать никаких просьб, предложений или разрешений на изменение цены или сути заявки;
- В случае если Участник Конкурса не предоставит соответствующие разъяснения его Конкурсной заявки или не представит запрашиваемые документы к сроку определения победителя Конкурса, его Конкурсная заявка может быть отклонена;
- Организатор Конкурса обязан отстранить Участника Конкурса от участия в Конкурсе, на любом этапе, в случае предоставления последним недостоверных сведений о его соответствии установленным требованиям.

17. **Условия оплаты**

- Оплата производится ОАО «Ориёнбонк»-ом по счету и по факту оказания услуг в течение **20 банковских дней с момента оказания услуг;**
- Все расчеты между покупателем и поставщиком осуществляются в **сомони**.
- Датой платежа считается дата списания средств со счета Заказчика.

18. **Порядок заключения договоров**

После утверждения Конкурсным комитетом ОАО «Ориёнбонк» итогов и победителей Конкурса, Организатор Конкурса публикует соответствующее уведомление на официальном сайте ОАО «Ориёнбонк».

ОАО «Ориёнбонк», пр. Рудаки 95/1,
г.Душанбе, ин.734001, Республика Таджикистан
Тел.: (37) 221-05-68; Факс: (37) 221-18-77
info@oriyonbonk.tj www.oriyonbonk.tj

ОРИЁНБОНК

Заявка на участие в конкурсе

Приложение 1
К конкурсной документации на поставку годовой лицензии программного обеспечения Kaspersky Endpoint Security for Business Advanced для ОАО «Ориёнбонк»

Участник_____
(полное наименование организации с указанием организационно-правовой формы) заявляет о своем намерении участвовать в открытом конкурсе на поставку годовой лицензии программного обеспечения Kaspersky Endpoint Security for Business Advanced для ОАО «Ориёнбонк»

1. соблюдать установленный законодательством Республики Таджикистан порядок проведения конкурса, а также условия конкурса, установленные организатором конкурса;
2. в случае признания победителем конкурса в установленный срок заключить договор на поставку лицензии программного обеспечения для ОАО «Ориёнбонк».

Место нахождения участника: _____
Почтовый адрес участника:
Контактный телефон участника:
Факс участника:
E-mail участника:
К заявке прилагаются документы в соответствии с требованиями конкурсной документации.
Приложение на _____ листах
Подпись участника (его полномочного представителя) _____
« » _____г.
К заявке прилагаются следующие документы, являющиеся ее неотъемлемой частью:

1. **выписка** из единого государственного реестра юридических лиц или нотариально заверенная копия такой выписки, надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица в соответствии с законодательством соответствующего государства (для иностранных лиц);
2. **документ,** подтверждающий полномочия лица на осуществление действий от имени участника размещения заказа, или нотариально заверенная копия такого документа;
3. **Предложение** о качестве услуг и иные предложения об условиях исполнения контракта, в том числе предложение о цене контракта, подписанное участником (его полномочным представителем).

Примечание: необходимо представить документы в запечатанных конвертах (опечатанных печатью Участника Конкурса) с указанием наименования подающих их компаний и наименования Конкурса.
Материалы, направленные в конвертах, оформленных ненадлежащим образом или полученные после указанного срока, рассматриваться не будут.

ОРИЁНБОНК

г.Душанбе, ин.734001, Республика Таджикистан
Тел.: (37) 221-05-68; Факс: (37) 221-18-77
info@oriyonbonk.tj www.oriyonbonk.tj

Заявка на участие в конкурсе

Приложение 2

Требования к предмету конкурса на поставку годовой лицензии программного обеспечения Kaspersky Endpoint Security for Business Advanced для ОАО «Ориёнбонк»

Общие требования

Антивирусные средства должны включать:

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

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.
Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.

Требования к программным средствам антивирусной защиты для рабочих станций Windows

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:
- Windows 7 Home / Professional / Enterprise (32 / 64-разрядная);
- Windows 8 Professional / Enterprise (32 / 64-разрядная);
- Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
- Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная);
- Windows 11 Home / Pro / Education / Enterprise (32 / 64-разрядная).

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:
- антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализации действий активного заражения;
- анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
- анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
- облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;

- фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
- проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, 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;
- 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 (ActiveDirectory 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 ActiveDirectory;
- возможность управления MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (ActiveDirectory 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 ActiveDirectory;
- защиты от атак типа BadUSB;
- запуск специальной задачи для обнаружения закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженнымуязвимостям.
- 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 файла, маске имени/директории или по наличию у файла доверенной цифровой подписи;
- наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
- наличие защищенного хранилища для отчетов о работе антивируса;
- возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей;
- возможностьинтеграциис Windows Defender Security Center;
- наличиеподдержки Antimalware Scan Interface (AMSI);
- наличиеподдержки Windows Subsystem for Linux (WSL);
- возможность защитить паролем восстановление объектов из резервного хранилища.
- полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии SingleSignOn, поддержка UEFI-систем;
- восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем;
- поддержка двухфакторной аутентификации при полнодисковом шифровании;
- шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению);
- наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля;
- шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
- возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);

Требования к программным средствам антивирусной защиты для серверов Windows

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

- Windows Small Business Server 2008 Standard / Premium (64-разрядная);
- Windows Small Business Server 2011 Essentials / Standard (64-разрядная);
- Windows MultiPoint Server 2011 (64-разрядная);
- Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная);
- Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная);
- Windows Server 2012 Foundation / Essentials / Standard (64-разрядная);
- Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная);
- WindowsServer 2016 (64-разрядная) (с ограничениями);
- WindowsServer 2019 (64-разрядная) (с ограничениями).

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

- антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализации действий активного заражения;
- анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
- анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
- облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
- создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (ActiveDirectory 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 прощенной версии графического интерфейса, с минимальным набором возможностей;
- возможностьинтеграциис Windows Defender Security Center;
- наличиеподдержки Antimalware Scan Interface (AMSI);
- наличиеподдержки Windows Subsystem for Linux (WSL);
- возможность защитить паролем восстановление объектов из резервного хранилища.

• возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);

Требования к программным средствам антивирусной защиты для рабочих станций Mac

Программные средства антивирусной защиты для рабочих станций Mac должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
○ macOS Catalina 10.15;
○ macOSMojave 10.14;
○ macOSHighSierra 10.13;
○ macOSSierra 10.12.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:
• резидентный антивирусный мониторинг;
• облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
• автоматическое обновление антивирусных баз по расписанию;
• резервное копирование зараженных файлов перед их удалением, для возможности восстановления;
• эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
• защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
• блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
• проверку сетевого трафика, передаваемого через браузеры Safari, GoogleChrome и Firefox (HTTP и HTTPS трафик);
• контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем
• ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
• централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault.

Требования к программным средствам антивирусной защиты для рабочих станций Linux

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 32-битных операционных систем следующих версий:
○ Ubuntu 16.04 LTS ивыше;
○ Red Hat® Enterprise Linux® 6.7 ивыше;
○ CentOS 6.7 и выше;
○ Debian GNU / Linux 9.4 и выше;
○ Debian GNU / Linux 10;

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 64-битных операционных систем следующих версий:
○ Ubuntu 16.04 LTS и выше;
○ Ubuntu 18.04 LTS и выше;
○ Red Hat Enterprise Linux 6.7 ивыше;
○ Red Hat Enterprise Linux 7.2 ивыше;
○ Red Hat Enterprise Linux 8.0 ивыше;
○ CentOS 6.7 и выше;
○ CentOS 7.2 и выше;
○ CentOS 8.0 и выше;
○ Debian GNU / Linux 9.4 и выше;
○ Debian GNU / Linux 10.1 и выше;
○ OracleLinux 7.3 и выше;
○ OracleLinux 8 и выше;

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:
• резидентного антивирусного мониторинга;
• облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
• проверку ресурсов доступных по SMB / NFS;
• возможность проверки памяти ядра;
• эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
• антивирусное сканирование по команде пользователя или администратора и по расписанию;
• антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
• проверку сообщений электронной почты в текстовом формате (Plaintext);

• наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
• защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
• возможность включения опции блокирования файлов во время проверки;
• помещение подозрительных и поврежденных объектов на карантин;
• проверку почтовых баз приложений MicrosoftOutlook на наличие вредоносных объектов;
• возможность перехвата и проверки файловых операций на уровне SAMBA;
• управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
• запуск задач по расписанию и/или сразу после загрузки операционной системы;
• возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
• гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
• сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
• возможность управления через пользовательский графический интерфейс без root прав;
• централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли.
• возможность управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения
• возможность проверки съемных дисков
• возможность отслеживания во входящем сетевом трафике активности, характерной для сетевых атак
• возможность проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым

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 MicrosoftWindows
○ Windows Server® 2003 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше;
○ Windows Server 2003 R2 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше;
○ Windows Server 2008 Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше;
○ Windows Server 2008 Core / Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше.

64-разрядныхоперационныхсистемMicrosoftWindows
○ Windows Server 2003 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше;
○ Windows Server 2003 R2 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше;
○ Windows Server 2008 Core Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше;
○ Windows Server 2008 Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше;
○ Microsoft Small Business Server 2008 Standard / Premium;
○ Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше;
○ Windows Server 2008 Core Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше;
○ WindowsHyper-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;
○ WindowsServer 2019/2022 Core;
○ WindowsStorageServer 2019/2022;
○ WindowsHyper-V Server 2019.

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

- антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
- защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
- непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям MicrosoftWindowsScriptTechnologies (или ActiveScripting), 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 MicrosoftWindows;
- 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 (ActiveDirectory или локальных пользователей/групп);
- компонентсоздания специальных правил должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
- компонентсоздания 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 ActiveDirectory;
- 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 программным средствам антивирусной защиты мобильных устройств

Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС:
- Android 4.2-10.0.
- iOS 10.0-13.0.
- iPadOS.

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
• блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
• поддержка белых списков разрешенных сайтов;
• наличие хранилища для изолирования зараженных объектов;
• обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;
• блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;
• поддержка белых списков разрешенных приложений;
• блокировка системных приложений, в рамках контроля запуска приложений;
• возможность отправки команд и push уведомлений через сервис FirebaseCloudMessaging (FCM);
• базовая поддержка AndroidforWork;
• возможность заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
• возможность указать параметры подключения к wi-fi сетям;
• возможность указать обязательные к установке приложения;
• возможность блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factoryreset);
• возможность создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
• поддержка технологий Samsung KNOX1 и KNOX2.

В программном средстве защиты смартфонов для ОС AppleiOS должны быть реализованы следующие функциональные возможности:
• возможность удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;
• возможность отправки команды блокирования и удаления данных;
• возможность создавать групповые политики безопасности мобильных устройств;
• удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу ExchangeActiveSync\ 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 supervisedmode;
• возможность централизованного управления с помощью единой консоли управления.

Требования к программным средствам централизованного управления, мониторинга и обновления

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
○ Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Pro длярабочихстанций RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Pro 19H1 32-разрядная / 64-разрядная;
○ MicrosoftWindows 10 Pro для рабочих станций 19H1 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Enterprise 19H1 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Education 19H1 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Pro 19H2 32-разрядная / 64-разрядная;
○ MicrosoftWindows 10 Pro для рабочих станций 19H2 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Enterprise 19H2 32-разрядная / 64-разрядная;
○ Microsoft Windows 10 Education 19H2 32-разрядная / 64-разрядная;
○ Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;
○ Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
○ Microsoft Windows 8 Pro 32-разрядная / 64-разрядная;
○ Microsoft Windows 8 Enterprise 32-разрядная / 64-разрядная;
○ Microsoft Windows 7 Professional Service Pack 1 32-разрядная / 64-разрядная;
○ Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-разрядная / 64-разрядная;
○ Windows Server 2019 Standard 64-разрядная;
○ Windows Server 2019 Standard 64-разрядная;
○ Microsoft Windows Server 2019 Datacenter 64-разрядная;
○ Microsoft Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-разрядная;
○ Microsoft Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-разрядная;
○ Microsoft Windows Server 2016 (вариантустановки Server Core RS3 (v1709) (LTSB/CBB) 64-разрядная;
○ Microsoft Windows Server 2016 Standard (LTSB) 64-разрядная;
○ Microsoft Windows Server 2016 (вариантустановки Server Core) (LTSB) 64-разрядная;

- Microsoft Windows Server 2016 Datacenter (LTSB) 64-разрядная;
- Microsoft Windows Server 2012 R2 Standard 64-разрядная;
- Microsoft Windows Server 2012 R2 Server Core 64-разрядная;
- Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
- Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
- Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 Standard 64-разрядная;
- Microsoft Windows Server 2012 Server Core 64-разрядная;
- Microsoft Windows Server 2012 Foundation 64-разрядная;
- Microsoft Windows Server 2012 Essentials 64-разрядная;
- Microsoft Windows Server 2012 Datacenter 64-разрядная;
- Microsoft Windows Storage Server 2016 64-разрядная;
- Microsoft Windows Storage Server 2012 R2 64-разрядная;
- Microsoft Windows Storage Server 2012 64-разрядная;

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:
- VMware vSphere 6.5;
- VMware vSphere 6.7;
- VMware Workstation 15 Pro;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;
- Microsoft Hyper-V Server 2019 64-разрядная;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Parallels Desktop 14;
- Oracle VM VirtualBox 6.x.

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:
- Microsoft SQL Server 2012 Express 64-разрядная;
- Microsoft SQL Server 2014 Express 64-разрядная;
- Microsoft SQL Server 2016 Express 64-разрядная;
- Microsoft SQL Server 2017 Express 64-разрядная;
- Microsoft SQL Server 2019 Express 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;
- 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;
- MySQL Standard Edition 5.7 32-разрядная / 64-разрядная;
- MySQL Enterprise Edition 5.7 32-разрядная / 64-разрядная;
- Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и MicrosoftAzure;
- MariaDBServer 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:
- выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
- возможность чтения информации из ActiveDirectory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
- возможность настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
- автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;
- централизованные установка, обновление и удаление программных средств антивирусной защиты;
- централизованная настройка, администрирование;
- просмотр отчетов и статистической информации по работе средств защиты;
- централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
- сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
- наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
- возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
- возможность иерархии триггеров, по которым происходит перераспределение;
- тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
- доставка обновлений на рабочие места пользователей сразу после их получения;
- распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;

- построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
- создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
- поддержка мультиарендности (multi-tenancy) для серверов управления;
- обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
- доступ к облачным серверам производителя антивирусного ПО через сервер управления;
- автоматическое распространение лицензии на клиентские компьютеры;
- инвентаризация установленного ПО и оборудования на компьютерах пользователей;
- наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
- функция управления мобильными устройствами через сервер ExchangeActiveSync;
- функция управления мобильными устройствами через сервер iOS MDM;
- возможность отправки SMS-оповещений о заданных событиях;
- централизованная установка сертификатов на управляемые мобильные устройства;
- возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
- возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
- построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
- наличие преднастроенных стандартных отчетов о работе системы;
- экспорт отчетов в файлы форматов PDF и XML;
- централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
- создание внутренних учетных записей для аутентификации на сервере управления;
- создание резервной копии системы управления встроенными средствами системы управления;
- поддержка Windows Failover Clustering;
- поддержкаинтеграциис Windows сервисом Certificate Authority;
- наличие веб-консоли управления приложением;
- наличие портала самообслуживания пользователей;
- портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
- наличие системы контроля возникновения вирусных эпидемий;
- возможность установки в облачной инфраструктуре MicrosoftAzure и GoogleCloud;
- возможность интеграции по OpenAPI;
- возможность управления антивирусной защитой с использованием WEB консоли.
- автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
- наличие преднастроенных ролей пользователей средств централизованного управления;
- 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;
- пользователю должен выводиться запрос на разрешение дистанционного подключения;
- наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (baremetal);
- должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;
- возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС;
- возможность импортировать образ операционной системы из дистрибутивов (WIM)
- наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии;
- автоматическое создание установочных пакетов для сторонних приложений (AdobeReader, MozillaFirefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры;
- поддержка функциональности управления шифрованием данных;
- возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF.

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:
- создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток;
- множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;
- проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к 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.
- 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.