УТВЕРЖДАЮ
Коммерческий директор по сбыту
_____Сыздыков К.Г.
«____» _____ 2021 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на приобретение услуг по предоставлению лицензий антивирусного программного обеспечения для нужд АО «МРЭК»

Описание объекта закупки

Общее количество лицензий- 250 шт.
Из них:
Персональные компьютеры – 240 шт.;
Серверы – 10 шт.

Общие требования

Антивирусная защита (АЗ) должна представлять собой масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети рабочих станций и серверов.

В рамках всей организации должны использоваться единые антивирусные средства. Отдельно стоящие персональные компьютеры, то есть не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от всех типов вредоносных программ (антивирус).

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке. Для организаций, имеющих офисы за границей, должна иметься возможность выбора языка интерфейса консоли управления для подключения к серверу администрирования, без переустановки консоли и сервера для ИТ персонала родной язык которого отличается от русского.

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

Технические параметры программных средств антивирусной защиты должны соответствовать или превосходить следующие указанные параметры:

Антивирусные средства и средства централизованного управления должны включать:

- лицензионные файлы ключей для пакетов антивирусного программного обеспечения (АПО); при использовании схемы с несколькими серверами удаленного администрирования кластерная технология для организации связи между серверами не требуется дополнительных лицензий на связь между серверами.
- программные средства антивирусной защиты рабочих станций, серверов и мобильных устройств (смартфонов, планшетов)
- агент администрирования для выполнения связи между сервером администрирования и защищаемыми узлами

- программные средства централизованного управления, мониторинга и обновления на ОС Windows, Linux/BSD, Mac OS, мобильные ОС Android;

- программные средства централизованного управления должны иметь WEB консоль для управления и формирования отчетов;
- централизованное управление может осуществляться с любого устройства через Web - браузер;
- программные средства централизованного управления могут устанавливаться на Windows и Linux платформы
- обновляемые антивирусные базы данных и компоненты ядра антивирусной системы;
- Прокси- сервер - компонент для обеспечения высокой масштабируемости решения и уменьшения нагрузки на центральный сервер администрирования
- наличие инструмента для обнаружения неизвестных компьютеров, осуществляющего автоматический поиск ПК в локальной сети, без необходимости осуществлять их ручной поиск и добавление;
- наличие различных вариантов установки агентов администрирования клиентской части антивирусного программного обеспечения такие как:
  удаленно или локально:
  - Push установка,
  - Установка через e-mail,
  - Установка с применением съемного носителя, например USB,
  - Локальная установка;
- эксплуатационную документацию на русском языке.

- Наличие выделенного программного инструмента для управления лицензиями. С его помощью можно отслеживать лицензии, активированные модули и связанные с лицензиями события, такие как окончание срока действия, использование и авторизация.

- Наличие выделенной утилиты для создания локального хранилища вирусных сигнатур, без использования сервера централизованного управления.

- Наличие возможности организации двухфакторной аутентификации пользователей консоли сервера централизованного управления.

- сервис дополнительного уровня безопасности продуктов, включающий встроенную песочницу

Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows

Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:

- Microsoft Windows Vista;
- Microsoft Windows Vista x64;
- Microsoft Windows 7
- Microsoft Windows 7 x64.
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:

- интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением;
- резидентный антивирусный мониторинг;
- возможность полностью скрыть интерфейс антивирусного ПО
- антивирусное сканирование по команде пользователя или администратора;
- антивирусное сканирование по расписанию;
- антивирусное сканирование при определенных условиях:
  - после обновлений антивирусных баз данных;
  - каждый раз при запуске компьютера;
  - каждые сутки при первом запуске компьютера;
  - при успешном Интернет или VPN соединении;
  - вход пользователя;
  - при обнаружении подозрительной активности, в том числе и активным модулем «защита в режиме реального времени».
  - состояние простоя, автоматически сканирует локальные диски, если компьютер находится в состоянии простоя, в одном из следующих трех режимов: заставка, блокировка компьютера, выход пользователя

- наличие задачи на выключение ПК по завершению сканирования
- антивирусное сканирование трафика по следующим протоколам: FTP, HTTP и HTTPs, POP3 и POP3s, а также IMAP и IMAPs трафика.
- наличие дополнительного модуля по защите документов Microsoft Office и сканировании проходящих через Internet Explorer файлов
- защита от еще неизвестных вредоносных программ на основе эвристического анализа;
- возможность добавлять в исключения только определенные угрозы, в независимости от их местонахождения на ПК:
- обнаружение скрытых процессов;
- возможность устанавливать только необходимые компоненты антивирусной защиты (модульная установка);
- возможность отключения антивирусной защиты при необходимости;
- антивирусная проверка и лечение файлов, упакованных программами типа *PKLITE, LZEXE, DIET, EXEPACK* и пр.;
- антивирусная проверка и лечение файлов в архивах форматов *ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE*;
- содержать настраиваемую систему предотвращения вторжений Host Intrusion Prevention System (HIPS) для предотвращения попыток внешнего воздействия, изменения, а также для мониторинга процессов, файлов и ключей реестра;
- возможность работы HIPS по ряду заранее подготовленных режимов фильтрации;
- обеспечивать защиту от хакерских атак, путем использования межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/HIPS) при работе в вычислительных сетях любого типа, включая беспроводные;
- персональный файервол;
- возможность настройки нескольких профилей файервола, с автоматическим переключением данных профилей, при выполнении определенных условий;

- управление всем сетевым трафиком компьютера в обоих направлениях;
- низкоуровневое сканирование трафика;
- поддержка протокола IPv6;
- поддержка встроенной песочницы для защиты от угроз нулевого дня;
- модуль сканирования UEFI;
- выделенный модуль защиты от вирусов шифраторов;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- возможность управления доступом к веб-ресурсам, путем создания списка заблокированных либо разрешенных веб-сайтов, а также путем запрета всех веб-сайтов, кроме тех, которые внесены в список разрешенных;
- активный режим фильтрации для приложений, а также возможность отключения фильтрации или перевод в пассивный режим для исключенных приложений;
- настраиваемый веб-контроль по категориям сайтов, позволяющий задавать правила применения политики использования сети Интернет на уровне пользователей или групп пользователей;
- Наличие в модуле веб-контроля возможности кастомизации страницы предупреждения или блокирования
- фильтрации для доверенных приложений;
- сканирование из контекстного меню;
- отключение фильтрации для доверенных веб-адресов;
- отключение фильтрации для доверенных IP адресов;
- возможность исключить из проверки доверенные процессы, хэш суммы, файлы и папки.
- настройка нескольких профилей обновлений (например, для мобильных пользователей) с возможностью обновления из сети Интернет;
- Наличие агента администрирования антивирусного программного обеспечения (АПО) для рабочих станций
- наличие планировщика в клиенте антивирусного ПО;
- возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы;
- ядро и все основные модули продукта не требуют перезагрузки и активны сразу после установки;
- наличие специализированной утилиты для сбора файлов журналов о конфигурации системы, установке и функционировании антивирусного пакета для ускорения решения проблем при возможных проблемах с антивирусным пакетом
- наличие модуля сканирования в состоянии простоя, автоматически сканирует локальные диски, если компьютер находится в состоянии простоя, в одном из следующих трех режимов: заставка, блокировка компьютера, выход пользователя
- возможность подключения уже установленных лицензий антивирусной защиты рабочих станций к серверу централизованного управления без необходимости удаления существующего пакета антивирусной защиты, путем установки агента администрирования;
- запуск обновления антивирусных баз данных после установки модемного соединения или VPN;

- возможность создания задачи запуска приложения стороннего производителя в планировщике антивируса при определенных условиях или по временному интервалу;
- защита на лету от вредоносных сценариев, загружаемых с Web-страниц
- блокирование нежелательных и рекламных сообщений
- самообучаемый антиспам;
- защита почтовых клиентов: Microsoft Outlook, Outlook Express,Windows Mail, Windows Live Mail;
- черные и белые списки антиспама, списки исключений
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- наличие функциональности использования общего локального кэша для повышения скорости сканирования в виртуализированных средах;
- защита от фишинга: защищает от попыток получить пароли и другую конфиденциальную информацию, запрещая доступ к вредоносным веб-сайтам, которые принимают вид нормальных веб-сайтов;
- Защита от эксплойтов: блокировщик эксплойтов контролирует поведение процессов и выявляет подозрительную активность, которая является типичной для целевых атак и ранее неизвестных эксплойтов – угроз нулевого дня
- наличие модуля сканирования памяти, который отслеживает поведение процессов и сканирует зловредные процессы, когда они снимают маскировку в памяти;
- защита от ботнетов: помогает обнаруживать вредоносные программы, анализируя их схемы обмена данными и протоколы
- регулировка распределения ресурсов рабочей станции между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме;
- настройка лимитов сканирования по параметрам – глубина вложенности (архивов), размера объекта и времени сканирования объекта;
- наличие модуля, позволяющего проводить автоматическое сканирование содержания подключаемых внешних устройств хранения данных, а также применять расширенный анализ для запуска файлов с таких устройств;
- наличие модуля, позволяющего настроить ограничения доступа (нет доступа, только чтение, полный доступ, предупреждение) для каждого пользователя или для группы пользователей как по типу устройства (CD/DVD/Blu-Ray, USB хранилища данных, USB принтеры, устройства обработки изображений, Устройства FireWire, кард ридеров, модемов, LPT\COM порты, Bluetooth устройства) так и по заданным атрибутам (производитель, модель, серийный номер) задавать одно правило на несколько устройств ;
- интеграция с MS NAP и CISCO NAC;
- возможность формирования аварийных дампов памяти, на случай сбоя приложения
- возможность отката обновлений вирусных баз на предыдущие версии и приостановка их обновления с последующим автоматическим включением обновления через указанный промежуток времени;
- наличие функциональности возобновлять прерванные загрузки баз данных сигнатур вирусов и модули продуктов при обновлении;
- интеграция с центром безопасности Windows;
- интеграция с центром обновления Windows, для установки патчей закрывающих обнаруженные уязвимости, с выбором необходимых обновлений от «необязательных» обновлений до «критических»;

- настройка проверки исполняемых файлов и загрузочных областей компьютера в качестве отдельной задачи;
- технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
- проверка наличия актуальных обновлений системы;
- наличие настраиваемой функции автоматического скрытия уведомлений при работе антивируса для приложений, работающих в полноэкранном режиме, т.е. при работе приложения в полноэкранном режиме на экран не выводятся информационные уведомления о работе антивирусного программного обеспечения;
- наличие множества путей уведомления администраторов о важных событиях, происходящих на рабочих станциях (почтовое сообщение, всплывающее окно, запись в журнал событий);
- обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на отчуждаемых носителях информации;
- экспорт логов и отчетов в форматы XML, TXT, DAT, DMP;
- наличие облачной технологии детектирования неизвестных угроз, контроль приложений на основе репутационного сервиса;
- наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную;
- возможность создания дисков аварийного восстановления;
- экономия электроэнергии в режиме автономного питания;
- системные требования не должны превышать: 300мб RAM, HDD 1гб, Processor Intel или AMD, одноядерный, x86 или x64 1ГГц.
- размер дистрибутива антивирусного пакета не должен превышать – 165 Мб.

Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows

Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:

- Microsoft Windows Server 2008 (x86 и x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2008 x64 R2 SP1 / x64 R2 CORE
- Microsoft Windows Server 2008 x86 SP2 / x64 SP2 CORE
- Microsoft Windows Server 2012 x64 / x64 CORE
- Microsoft Windows Server 2012 x64 R2 / x64 R2 CORE
- Microsoft Windows Hyper-V Server 2008 R2
- Microsoft Windows Hyper-V Server 2012
- Microsoft Windows Hyper-V Server 2012 R2

Серверы Storage, Small Business и MultiPoint:

- Microsoft Windows Storage Server 2008 R2 Essentials с пакетом обновления 1
- Microsoft Windows Storage Server 2012
- Microsoft Windows Storage Server 2012 R2

- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows MultiPoint Server 2010
- Microsoft Windows MultiPoint Server 2011
- Microsoft Windows MultiPoint Server 2012

Программные средства антивирусной защиты файловых серверов под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:

- интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением;
- резидентный антивирусный мониторинг;
- антивирусное сканирование по команде пользователя или администратора;
- антивирусное сканирование по расписанию;
- антивирусное сканирование при определенных условиях:
  - после обновлений антивирусных баз данных;
  - каждый раз при запуске компьютера;
  - каждые сутки при первом запуске компьютера;
  - при успешном Интернет или VPN соединении;
  - вход пользователя;
  - при обнаружении подозрительной активности, в том числе и активным модулем «защита в режиме реального времени».
- антивирусное сканирование трафика по следующим протоколам: FTP, HTTP и HTTPs, а также POP3 и POP3s трафика
- антивирусное сканирование Hyper-V на наличие вирусов на безагентной основе
- защита от еще неизвестных вредоносных программ на основе эвристического анализа;
- содержать настраиваемую систему предотвращения вторжений Host Intrusion Prevention System (HIPS) для предотвращения попыток внешнего воздействия, изменения, а также для мониторинга процессов, файлов и ключей реестра;
- возможность работы HIPS по ряду заранее подготовленных режимов фильтрации
- возможность добавлять в исключения только определенные угрозы, в независимости от их местонахождения на ПК:
- возможность исключить определенные процессы приложений, хэш суммы из сканирования на наличие вирусов;
- обнаружение руткитов (скрытых файлов/системных аномалий);
- антивирусная проверка и лечение файлов, упакованных программами типа *PKLITE, LZEXE, DIET, EXEPACK* и пр.;
- антивирусная проверка и лечение файлов в архивах форматов *ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE*;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- возможность создания задачи запуска приложения стороннего производителя в планировщике антивируса;
- защита на лету от вредоносных сценариев, загружаемых с Web-страниц;
- возможность настройки параметров антивирусного пакета из интерфейса командной строки

- функция автоматического обнаружение и исключения файлов на сервере, имеющих критическое значение для бесперебойной работы;
- возможность задать количество модулей сканирования для увеличения скорости сканирования;
- возможность управления доступом к веб-ресурсам, путем создания списка заблокированных либо разрешенных веб-сайтов, а также путем запрета всех веб-сайтов, кроме тех, которые внесены в список разрешенных;
- активный режим фильтрации для приложений, а также возможность отключения фильтрации или перевод в пассивный режим для исключенных приложений;
- сканирование из контекстного меню;
- отключение фильтрации для доверенных веб-адресов;
- многопоточное сканирование;
- настройка нескольких профилей обновлений (например, для мобильных пользователей) с возможностью обновления из интернета.
- наличие планировщика в антивирусном пакете.
- наличие агента администрирования антивирусного программного обеспечения (АПО) для файловых серверов
- возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы;
- ядро и все основные модули продукта не требуют перезагрузки и активны сразу после установки;
- возможность подключения уже установленных лицензий антивирусной защиты рабочих станций к серверу централизованного управления без необходимости удаления существующего пакета антивирусной защиты, путем установки агента администрирования;
- наличие облачной технологии детектирования неизвестных угроз, контроль приложений на основе репутационного сервиса;
- запуск обновления антивирусных баз после установки модемного соединения или VPN;
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- наличие специализированной утилиты для сбора файлов журналов о конфигурации системы, установке и функционировании антивирусного пакета для ускорения решения проблем при возможных проблемах с антивирусным пакетом
- наличие функциональности использования общего локального кэша для повышения скорости сканирования в виртуализированных средах;
- защита от фишинга: защищает от попыток получить пароли и другую конфиденциальную информацию, запрещая доступ к вредоносным веб-сайтам, которые принимают вид нормальных веб-сайтов;
- Защита от эксплойтов: блокировщик эксплойтов контролирует поведение процессов и выявляет подозрительную активность, которая является типичной для целевых атак и ранее неизвестных эксплойтов – угроз нулевого дня
- поддержка встроенной песочницы для защиты от угроз нулевого дня;
- модуль сканирования UEFI;

- выделенный модуль защиты от вирусов шифраторов;
- модуль защиты от сетевых атак;
- модуль защиты от ботнетов;
- наличие модуля сканирования памяти, который отслеживает поведение процессов и сканирует зловредные процессы, когда они снимают маскировку в памяти;
- регулировка распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме;
- настройка лимитов сканирования по параметрам – глубина вложенности (архивов), размера объекта и времени сканирования объекта;
- блокировка сменных носителей информации и устройств (USB);
- наличие модуля, позволяющего настроить ограничения доступа (нет доступа/только чтение/полный доступ/предупреждение) для каждого пользователя или для группы пользователей как по типу устройства (CD/DVD/Blu-Ray, USB хранилища данных, USB принтеры, устройства обработки изображений, Устройства FireWire, кард ридеров, модемов, LPT\COM порты, Bluetooth устройства) так и по заданным атрибутам (производитель/модель/серийный номер) задавать одно правило на несколько устройств ;
- интеграция с центром безопасности Windows;
- интеграция с центром обновления Windows, для установки патчей закрывающих обнаруженные уязвимости, с выбором необходимых обновлений от «необязательных» обновлений до «критических»;
- поддержка Windows Management Instrumentation
- настройка проверки исполняемых файлов и загрузочных областей компьютера в качестве отдельной задачи;
- поддержка кластерных систем с возможностью автоматического объединения антивирусного ПО (автоматическая синхронизация конфигурации ПО на кластерах)
- технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
- проверка наличия актуальных обновлений операционной системы;
- полноценная работа без графического интерфейса, администрирование и конфигурирование АПО через командную строку;
- возможность автоматизации работы за счет выполнения сценариев, позволяющих конфигурировать АПО и выполнять какие-либо действия;
- автоматическое скрытие уведомлений при работе антивируса в полноэкранном режиме;
- наличие настраиваемой функции автоматического скрытия уведомлений при работе антивируса для приложений, работающих в полноэкранном режиме;
- наличие множества путей уведомления администраторов о важных событиях, происходящих на серверах (почтовое сообщение, всплывающее окно, запись в журнал событий);
- обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на отчуждаемых носителях информации;
- наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную;
- возможность создания дисков аварийного восстановления;
- размер дистрибутива антивирусного пакета не должен превышать – 127 Мб.

Требования к средствам антивирусной защиты мобильных устройств

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

Android 4 (Ice Cream Sandwich) и выше

Программные средства антивирусной защиты смартфонов должны обеспечивать следующую функциональность:

- возможность проведения аудита безопасности устройства с генерацией отчета;
- постоянная защиту файловой системы смартфона, планшета;
- проверка всех приложений, файлов, папок и карты памяти в режиме реального времени;
- проверка объектов файловой системы, находящихся на смартфоне или на подключенных картах расширения памяти, по требованию пользователя и по расписанию;
- надежное изолирование зараженных объектов в карантинном хранилище;
- обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов;
- блокирование нежелательных SMS и MMS сообщений;
- контроль приложений для отслеживания установленных приложений, блокировать доступ к определенным приложениям и снижать степень риска, предлагая пользователям удалять некоторые программы
- задание минимальных уровней безопасности и сложность кодов разблокировки экрана;
- указание максимального количества неудачных попыток разблокировки;
- указание максимального срока действия для кода разблокировки экрана;
- настройка таймера блокировки экрана;
- ограничить использование камеры.
- защита от фишинга: защита пользователей от попыток получить пароли, банковские данные и прочую конфиденциальную информацию незаконными веб-сайтами, выдающими себя за законные
- центр уведомлений: предоставляет сведения о разных событиях, о причинах их несоответствия корпоративным политикам и о том как эту несовместимость устранить
- защита от кражи и утери смартфона. Обеспечить возможность удаленной блокировки мобильного устройства;
- возможность дистанционно удалить информацию со смартфона;
- возможность определить доверенную SIM-карту;
- автоматическая скрытая отправка уведомления посредством SMS-сообщения, с предупреждением об использовании не доверенной SIM-карте. Так же сообщение должно включать информацию, необходимую для идентификации злоумышленника: телефонный номер текущей SIM-карты, номер IMSI и номер IMEI телефона.
- расширенный сброс до заводских установок: все доступные на устройстве данные будут удалены (заголовки файлов будут уничтожены). Кроме того, на телефоне будут восстановлены заводские настройки по умолчанию
- возможность включить сирену: отерянное устройство блокируется и начинает издавать очень громкий звук, даже если звук на устройстве отключен
- Наличие встроенного агента администрирования антивирусного программного обеспечения (АПО)
- Системные требования: Операционная система: Android 4 (Ice Cream Sandwich) и более поздние версии. Разрешение сенсорного экрана: 480 x 800 пкс. Процессор: ARM с набором инструкций ARMv7. Свободное место для хранения данных: 20 МБ.

Требования к системе управления антивирусной защитой

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

- масштабируемое решение: масштабирование производится за счет использования прокси серверов
- интерфейс антивирусного программного обеспечения должен обеспечивать поддержку сенсорных экранов и экранов с высоким разрешением;
- Прокси- сервер - компонент для обеспечения высокой масштабируемости решения и уменьшения нагрузки на центральный сервер администрирования
- наличие инструмента для обнаружения неизвестных компьютеров, осуществляющий автоматический поиск ПК в локальной сети, без необходимости осуществлять их ручной поиск и добавление;
- централизованная установка/обновление/удаление программных средств антивирусной защиты, настройки, администрирования;
- централизованный сбор информации и создание отчетов о состоянии антивирусной защиты;
- защищенное соединение между сервером и клиентом;
- программные средства централизованного управления должны иметь WEB консоль для управления и формирования отчетов;
- централизованное управление может осуществляться с любого устройства через Web - браузер;
- создание отчетов в наглядном графическом виде;
- экспорт логов и отчетов в форматы HTML, TXT, CSV, PDF;
- наличие модуля поддержки SIEM;
- предварительная настройка политик для групп или клиентов (профили обновлений, запрещенные сайты, расписание планировщика и т.д.);
- возможность отправки сообщений, как на мобильные устройства, так и на персональные компьютеры;
- возможность удаленного создания журнала аудита безопасности с мобильного устройства
- возможность установки пользовательских приложений;
- наличие различных вариантов установки агентов администрирования клиентской части антивирусного программного обеспечения такие как:
  удаленно или локально:
  - Push установка,
  - Установка через e-mail,
  - Установка с применением съемного носителя, например USB,
  - Локальная установка;
- наличие возможности автоматически выбирать соответствующий установочный пакет агента для операционных систем или в ручном режиме.
- настройка политик безопасности для клиентов;
- возможность централизованно посмотреть общую информацию о состоянии ПК, об установленных приложениях, службах, сетевых подключениях и т.д. с возможностью отслеживания изменений и их автоматического сравнения с помощью снимков по временному интервалу, а так же возможность внесения изменений (остановка процессов и драйверов, удаление и восстановление записей реестра и системных файлов) восстанавливающих корректную работу системы;
- возможность удаленного запуска определенного сценария на конечных клиентах, предназначенного для удаления/изменения критических объектов системы.

- отсутствие необходимости перезагрузки ПК после установки системы управления антивирусной защиты;
- автоматизированное обновление программных средств антивирусной защиты и антивирусных баз;
- возможность произвести быстрый откат обновлений сигнатурных баз для отдельных компьютеров или групп;
- доставка обновлений на рабочие места пользователей сразу после их получения;
- централизованный карантин;
- возможность создания групп управляемых компьютеров как вручную, так и автоматически на основе структуры Active Directory;
- возможность синхронизации с Active Directory как по расписанию, так и вручную;
- автоматический поиск незащищенных рабочих станций с учетом топологии сети;
- аудит изменений в настройках сервера по учетным записям;
- построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
- обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на носителях информации;
- механизм оповещения о событиях в работе установленных приложений антивирусной защиты и возможность настройки рассылки почтовых уведомлений о них;
- наличие системы передачи образцов вредоносного кода вирусным экспертам автоматически или вручную;
- возможность создания динамических групп, в которые динамически будут включаться клиентские станции при соответствии условиям данных групп;
- работа со статическими и динамическими группами
- различные варианта уведомлений администратора сети (по e-mail, использование SNMP-ловушки);
- возможность создания резервных копий содержимого базы данных и настроек сервера;
- возможность подключения к консоли сервера удаленного администрирования с использованием доменных имени пользователя и пароля;
- администрирование серверов и рабочих станций Windows, Linux\BSD, а также решений для защиты мобильных ОС (Android);
- наличие функции пробуждения по локальной сети Wake on LAN
- возможность автоматического определения «клонированных машин» с помощью сложной логики обнаружения отпечатков оборудования.
- наличие протокола для репликации, с использованием «PNS» (Push Notification Service) и поддержкой многоадресных вызовов для WOL.
- функционал для инвентаризации оборудования.
- наличие функции быстрого отключения или включения уведомлений на выбранных компьютерах для прерывания или возобновления обмена данными с сервером администрирования
- поддержка баз данных MS SQL, MySQL;
- программные средства централизованного управления могут устанавливаться на Windows и Linux платформы
- программные средства должны поддерживать установку на отказоустойчивые кластеры Windows и Linux платформ
- сервер удаленного администрирования может быть установлен и должен поддерживать операционные системы
  Windows Server:
  - Windows Server 2003 x86 SP2 /x64 SP2
  - Windows Server 2003 x86 R2 SP2 /x64 R2 SP2
  - Windows Server 2008 x64 R2 SP1 / x64 R2 CORE
  - Windows Server 2008 x86 SP2 / x64 SP2

- Windows Server 2012 x64 / x64 CORE
- Windows Server 2012 x64 R2 / x64 R2 CORE
- Microsoft SBS 2003 x86 SP2 / x86 R2
- Microsoft SBS 2008 x64 SP2
- Microsoft SBS 2011 x64 Standard / x64 Essential

Linux:

- Ubuntu 12.04 LTS x86 Desktop / Server
- Ubuntu 12.04 LTS x64 Desktop / Server
- Ubuntu14.04. LTS x86 Desktop / Server
- Ubuntu 14.04 LTS x64 Desktop / Server
- RHEL Server 6 x86 / x64
- RHEL Server 7 x86 / x64
- CentOS 6 x86 / x64
- CentOS 7 x86 / x64
- SLED 11 x86 / x64
- SLES 11 x86 /x64
- OpenSUSE 13 x86 / x64
- Debian 7 x86 / x64
- Fedora 19 x86 / x64

- Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий:
  - VMware vSphere/ESXi (версии 5.0 и новее)
  - VMware Workstation (версии 9 и новее)
  - VMware Player (версии 7 и новее)
  - Microsoft Hyper-V (Server 2012 и 2012 R2)
  - Oracle VirtualBox (версии 4.3.24 и новее)

Наличие выделенного программного инструмента для управления лицензиями. С его помощью можно отслеживать лицензии, активированные модули и связанные с лицензиями события, такие как окончание срока действия, использование и авторизация. Работа с инструментом под разными ролями как владелец лицензии или как администратор безопасности.
Возможность выполнять следующие действия:

- просматривать состояние лицензий в реальном времени;
- отслеживать отдельные устройства (и при этом их отключать);
- настраивать уведомления, связанные с событиями лицензии;
- хранить лицензии одновременно в старой и новой формах в смешанных средах;
- обменивать ключи лицензий на сообщения электронной почты и пароли, с помощью которых также можно активировать программы;
- назначать несколько лицензий на одну учетную запись;
- разрешать другим лицам использовать лицензии (активировать их);
- настраивать уведомления для более удобного отслеживания состояния лицензии;
- наличие функции синхронизации с сервером централизованного управления.
- наличие выделенной утилиты для мигрирования с более ранних версий антивирусного программного обеспечения с сохранением настроек политик и информационной базы журналов событий.
- наличие выделенной утилиты для создания локального хранилища вирусных сигнатур, без использования сервера централизованного управления.

- наличие возможности организации двухфакторной аутентификации пользователей консоли сервера централизованного управления. Поддержка двухфакторной аутентификации для 10 пользователей консоли сервера централизованного управления. При использовании данной функциональности должно быть использовано решение двухфакторной аутентификации того же производителя, что и сам пакет антивирусного программного обеспечения.

- наличие возможности деактивации лицензий на узлах через создание заданий на сервере управления.

Сервис дополнительного уровня безопасности продуктов для защиты рабочих станций, файловых и почтовых серверов с помощью встроенной песочницы на основе технологий машинного обучения для обнаружения новых, ранее неизвестных угроз.

В сервисе должна быть реализована следующая функциональность:

- Детектирование на основе анализа поведения
- Машинное обучение
- Обнаружение угроз нулевого дня
- Встроенная песочница

Сервис на основе технологий машинного обучения для обнаружения новых, ранее неизвестных угроз поставляется в составе решения по антивирусной защите рабочих станций, файловых серверов локальной сети заказчика.

- Наличие поддержки антивирусными продуктами дополнительной функциональности, активируемой отдельной лицензией. Сервис предназначен для продуктов того же производителя антивирусного обеспечения, что и сам сервис. Сервис должен активироваться и управляться из центра обеспечения безопасности системы.
- Сервис должен поддерживать работу с антивирусными решениями по защите рабочих станций, файловых серверов и почтовых серверов.
- Для работы с сервисом необходим только доступ в сеть интернет, никаких аппаратных средств в сети заказчика не требуется.

Сервис должен обеспечивать:

- Многоуровневую защиту - иметь не менее 3 моделей машинного обучения. Система выполняет работу с образцами в виртуальной среде или в песочнице. Система моделирует поведение пользователей, чтобы обмануть образцы вредоносных программ и использует модели нейронных сетей Deep Learning для сравнения поведения образцов с поведением всех известных образцов вредоносных программ.
- Детальный обзор - Каждый изучаемый образец отображается в консоли центра безопасности, где наглядно и удобно представлена детальная информация о его характеристиках и происхождении.
- Высокую скорость анализа – предоставлять анализ 90% неизвестных образцов в течение 5 минут
- Мобильность – наличие возможности анализа файлов вне зависимости от местонахождения пользователей в корпоративной сети или за ее пределами.
- Наличие возможности отправки подозрительных файлов вручную или автоматически на основе конфигурации политики.
- Возможность отправки файлов вручную из веб-консоли Центра обеспечения безопасности или с клиентских компьютеров с активированным сервисом.
- Возможность управлять действиями сервиса через API Центра обеспечения безопасности
- Наличие возможности отправки больших файлов объемом до 64 Мб
- Поддерживаемые типы файлов для отправки на проверку:
  - Документы (.docx, .xslx, .rtf и др.)
  - Исполняемые файлы (файлы .exe, .dll, .sys и др.)

- JAR, LNK, REG, MSI, SWF и др
- Сценарии (.bat, .cmd, .js, .vbs, .ps и др.)
- Ole2 - при использовании с продуктами по защите почтовых серверов
- .hta

- Наличие функциональности предоставления отчета о поведении проверенного образца, в котором будет приведено краткое описание поведения наблюдаемого образца.

В Отчете о файле должна содержаться следующая информация:

- Имя компьютера, отправившего файл
- указание Пользователя на исходном компьютере, отправившего файл. В некоторых случаях это может быть системный пользователь
- Причина отправки (автоматически, вручную).
- указана Часть облака, получившая файл
- Хеш SHA1 отправленного файла.
- Имя файла и его полный путь в файловой системе отправителей.
- Размер файла.
- Категория файла (тип файла).

- Наличие в отчете параметров: **Состояние** и **Статус**:
  - **Состояние** означает текущее состояние файла в процессе выполнения анализа
  - **Статус** означает результат анализа поведения или отсутствие результата
- Наличие категории статуса, присвоенного проверенным образцам, которое отображается в консоли центра управления или в отчете по образцу:
  - **Не заражено** - Модули обнаружения не идентифицируют образец как вредоносный.
  - **Подозрительный** - Модуль обнаружения определил поведение файла как подозрительное, но не вредоносное.
  - **Вредоносный** - Поведение файла считается вредоносным.
- Наличие функциональности распространения результатов о проверенных файлах во все продукты для обеспечения безопасности в компании пользователя в течение не более 2 минут
- Наличие функциональности предоставления списка о всех переданных файлах в консоль Центра обеспечения безопасности. Можно просмотреть список отправленных файлов в выделенном разделе консоли.
- Возможность настройки отправки образцов в консоли Центра обеспечения безопасности
- Возможность настройки исключений для образцов и настройки политик для продуктов обеспечения безопасности в консоли Центра обеспечения безопасности.

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

- реализована возможность создания зеркала обновлений для экономии трафика;
- зеркало обновлений можно создать на любом ПК сети не зависимо от используемой операционной системы Windows/Linux, в том числе и на конечной рабочей станции при помощи AV-клиента с обязательным наличием как минимум двух путей раздачи обновлений (HTTP и SMB), для активации зеркала не должна требоваться установка дополнительных модулей, как на сервер, так и на рабочую станцию;
- типы обновлений: обновление БД сигнатур вирусов, программных компонентов, обновление ядра;
- пакеты обновления зеркала можно загружать двумя способами: по протоколу HTTP (рекомендуется) и с помощью общего сетевого диска (SMB);
- обновления можно распространять на электронных носителях информации (FDD\CD\DVD\ USB-drive);

- осуществляется проверка 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 на русском языке, в том числе:

- руководство пользователя (администратора);
- руководство администратора средств удаленного администрирования.

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 на всей территории Республики Казахстан круглосуточно без праздников и выходных (24х7) по электронной почте и через Интернет, а также по телефону;
- Web-сайт производителя АЗ должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний и русскоязычный форум.

Место и сроки оказания услуг

С момента заключения договора по 31 декабря 2021 года.
Мангистауская область 130000, город Актау, 29А микрорайон,
здание №97 (район птицефабрики).

Начальник отдела
информационных технологий **Е.Балтабаев**