ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на закупку права на использование обновления   
антивирусного программного средства

Поставщик обязуется поставить права на использование обновления антивирусного программного средства из состава продуктов ЗАО «Лаборатория Касперского», которые внедрены и используются в учреждении по следующим позициям и удовлетворяющего следующим характеристикам:

1. **Права на компьютерную программу «Kaspersky Endpoint Security   
   for Business – Select», продление 900 лицензий, срок действия 12 месяцев.**
   1. Антивирусные средства должны включать:
      * программные средства антивирусной защиты для рабочих станций Windows;
      * программные средства антивирусной защиты для файловых серверов Windows;
      * программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows;
      * программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов);
      * программные средства централизованного управления, мониторинга   
        и обновления;
      * обновляемые базы данных сигнатур вредоносных программ и атак;
      * эксплуатационную документацию на русском языке;

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

* 1. Требования к программным средствам антивирусной защиты для рабочих станций Windows.

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

* + - Microsoft Windows 7 Professional/Enterprise/Ultimate x86/x64;
    - Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 и выше x86/x64;
    - Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
    - Microsoft Windows 10 Professional / Enterprise x86 / x64;
    - Microsoft Windows 11.

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

* + - резидентный антивирусный мониторинг;
    - защита от программ-маскировщиков, программ автодозвона на платные сайты;
    - эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
    - антивирусное сканирование по команде пользователя   
      или администратора и по расписанию;
    - запуск задач по расписанию и/или сразу после загрузки операционной системы;
    - антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем;
    - защита электронной корреспонденции от вредоносных программ   
      с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP — независимо от используемого почтового клиента;
    - защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных сайтов;
    - блокировка баннеров и всплывающих окон, загружаемых с Web-страниц;
    - распознавание и блокировка фишинг-сайтов;
    - проверка трафика ICQ и MSN, для обеспечения безопасности работы   
      с интернет-пейджерами;
    - защита от еще не известных вредоносных программ на основе анализа их поведения;
    - возможность определения аномального поведения приложения   
      с помощью анализа последовательности действий этого приложения. возможность совершить откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных вредоносными программами файлов;
    - возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы;
    - наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ;
    - 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;
    - наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме MD5, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, а также обеспечивать возможность исключения из правил для определенных пользователей из Active Directory;
    - осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине,   
      с возможностью создания списка доверенных устройств   
      по их идентификатору и возможностью предоставления привилегий   
      для использования внешних устройств определенным пользователям   
      из Active Directory;
    - осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки определенного типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
    - ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
    - запуск специальной задачи для обнаружения уязвимостей   
      в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
    - гибкое управление использованием ресурсов компьютера   
      для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
    - защита 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;
    - возможность установки только выбранных компонентов программного средства антивирусной защиты;
    - централизованное управление всеми вышеуказанными компонентами   
      с помощью единой системы управления.
  1. Требования к программным средствам антивирусной защиты для файловых серверов Windows.

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

* + - Microsoft Windows Server 2003 Standard/Enterprise SP2 x32/x64;
    - Microsoft Windows Server 2003 R2 Standard/Enterprise Edition SP2 R2 x32/x64;
    - Microsoft Windows Server 2008 R2 x64 Standard/Enterprise SP1 и выше;
    - Microsoft Windows Server 2012 R2 Standard/Essentials х64 Edition;
    - Microsoft Windows Server 2016;
    - Microsoft Windows Server 2019;
    - Microsoft Windows Server 2022.

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

* + - резидентный антивирусный мониторинг;
    - эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
    - антивирусное сканирование по команде пользователя   
      или администратора и по расписанию;
    - запуск задач по расписанию и/или сразу после загрузки операционной системы;
    - наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ:
    - 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;
    - запуск специальной задачи для обнаружения уязвимостей   
      в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
    - антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем;
    - ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
    - 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);
    - защита 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;
    - централизованное управление всеми вышеуказанными компонентами   
      с помощью единой системы управления.
  1. Требования к программным средствам антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows.

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

* + - Microsoft Windows Server 2003 Standard/Enterprise x32/x64 SP2 или выше;
    - Microsoft Windows Server 2003 R2 Standard/ Enterprise Edition x32/x64 SP2 и выше;
    - Microsoft Windows Server 2008 Standard / Enterprise /DataCenter x32/x64 SP1 и выше;
    - Microsoft Windows Server 2008 R2 Standard/ Enterprise/ DataCenter x64 SP1 или выше;
    - Microsoft Windows Server 2016;
    - Microsoft Windows Server 2019;
    - Microsoft Windows Server 2022;
    - Microsoft Windows Hyper-V Server 2008 R2 SP1 или выше;
    - Microsoft Windows Server 2012 R2 Standard/ Essential/ DataCenter/Foundation;
    - Microsoft Windows Hyper-V Server 2012 R2;
    - Microsoft Windows Hyper-V Server 2019;
    - Microsoft Remote Desktop Services на базе Windows Server 2008 SP2 или выше;
    - Microsoft Remote Desktop Services на базе Windows Server 2008 R2;
    - Microsoft Remote Desktop Services на базе Windows Server 2012 R2;
    - Microsoft Remote Desktop Services на базе Windows Server 2016;
    - Microsoft Remote Desktop Services на базе Windows Server 2019;

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

* + - осуществление антивирусной проверки на серверах, выполняющих разные функции: Серверов терминалов; Серверов приложений   
      и контроллеров доменов; Файловых серверов;
    - возможность использования для защиты кластера серверов;
    - проверка следующих объектов защищаемого сервера при доступе к ним: Файлов при их записи и считывании; Альтернативных потоков файловых систем (NTFS-streams); Главной загрузочной записи и загрузочных секторов локальных жестких дисков и съемных носителей;
    - предотвращение вирусных эпидемий за счет фиксации возникновения вирусных атак;
    - восстановление после заражения путем удаления всех связанных   
      с ликвидированным вредоносным объектом записей в системных файлах и реестре ОС, что предотвращает возможные сбои в работе операционной системы;
    - непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting). Проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными;
    - проверка по требованию, заключающаяся в однократной полной или выборочной проверке на наличие угроз объектов на сервере;
    - проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
    - помещение подозрительных и поврежденных объектов на карантин. возможность восстановления файлов из карантина в сетевые папки;
    - при защите терминальных серверов поддержка режимов публикации рабочего стола и публикации приложений;
    - масштабируемость за счет задания количества рабочих процессов антивируса для ускорения обработки запросов к серверу   
      при использовании многопроцессорных серверов;
    - балансировка загрузки путем регулирования распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: антивирусная проверка может продолжаться в фоновом режиме;
    - выбор доверенных процессов путем исключения из проверки безопасных процессов, работа которых может замедляться при антивирусной проверке (процесс резервного копирования данных, программы дефрагментации жесткого диска и другие);
    - разделение прав администраторов, основанное на стандартных механизмах ОС Microsoft Windows;
    - наличие встроенных исключений для стандартных ролей сервера (Контролер домена, Сервер БД и тд);
    - уведомления различными методами администраторов и пользователей   
      о событиях в антивирусной защите. Поддержка Simple Network Management Protocol (SNMP);
    - запуск задач по расписанию и или сразу после загрузки операционной системы;
    - наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов,   
      а также позволяющего создавать сетевые правила для конкретных программ;
    - 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;
    - запуск специальной задачи для обнаружения уязвимостей   
      в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
    - проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB   
      в том числе и защищенных паролем;
    - настройки проверки критических областей сервера в качестве отдельной задачи;
    - защита 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.
    - централизованно управляться с помощью единой системы управления.
  1. Требования к программным средствам антивирусной защиты мобильных устройств.

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

* + - Android 5.0 – 12;
    - Apple iOS 10.0 – 15.

Решение должно централизованно управлять с помощью единой консоли управления.

Программные средства для антивирусной защиты смартфонов для ОС Android должны обеспечивать следующую функциональность:

* + - постоянная антивирусная защита файловой системы смартфона,   
      с дополнительным уровнем проверки на репутационных облачных сервисам производителя антивирусных средств защиты. Мгновенная проверка устанавливаемых приложений. Проверка файловой системы устройства по требованию и по раcсписанию;
    - 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;
    - возможность получения политик безопасности через Google Cloud Messaging;
    - наличие возможности создания специальной оболочки для мобильных программ с целью контроля действий программы, возможностью удаления данных и настроек программы, добавления дополнительного пароля для старта приложения, в том числе с помощью учетных данных Active Directory;
    - возможность заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
    - указание параметров подключения к wi-fi сетям;
    - наличие возможности указания обязательных к установке приложений;
    - блокирование нежелательных SMS сообщений;
    - возможность блокировки мобильного устройства, удаление данных, удаление данных, связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата   
      к заводским настройкам (factory reset);
    - постоянная проверка телефона на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий. Возможность получения текущего номера SIM-карты телефона посредством СМС, возможность автоматической блокировки устройства при смене SIM-карты или при включении телефона без SIM-карты;
    - поддержка технологий Samsung KNOX1 и KNOX2.

Программные средства для антивирусной защиты смартфонов для ОС Apple iOS должны обеспечивать следующую функциональность:

* + - блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
    - возможность определения местоположения устройства;
    - наличие возможности создания специальной оболочки для мобильных программ с целью контроля действий программы, возможностью удаления данных и настроек программы, добавления дополнительного пароля для старта приложения, в том числе с помощью учетных данных Active Directory.
  1. 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 7 Professional/Enterprise/Ultimate x86/x64;
    - Microsoft Windows 10 Pro/Enterprise 19H1/20H1/21H2 x86/x64;
    - Microsoft Windows Server 2008 R2;
    - Microsoft Windows Server 2012 R2;
    - Microsoft Windows Server 2016;
    - Microsoft Windows Server 2019;
    - Microsoft Windows Server 2022.

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

* + - Microsoft SQL Express 2012/2014/2016/2019;
    - Microsoft SQL Server 2012/2014/2016/2019;

Программные средства централизованного управления, мониторинга   
и обновления должны функционировать на виртуальных платформах Microsoft Hyper-V: 2012, 20012 R2, 2016

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

* + - установка системы управления антивирусной защиты из единого дистрибутива;
    - выбор установки в зависимости от количества защищаемых узлов;
    - возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров в организации;
    - возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети;
    - 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 Organization Units Active Directory;
    - централизованные установка, обновление и удаление программных средств антивирусной защиты. Настройка, администрирование, просмотр отчетов и статистической информации по их работе;
    - централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
    - наличие различных методов установки антивирусных агентов:   
      для удаленной установки - RPC, GPO, агент администрирования,   
      для локальной установки – возможность создать автономный пакет установки;
    - централизованная установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации   
      по их работе;
    - возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от ученой записи, под которой пользователь вошел   
      в систему, а также от того, в каком Organization Units находится компьютер. Должна быть реализована возможность поддержки иерархии таких триггеров;
    - автоматизированное обновление программных средств антивирусной защиты и антивирусных баз;
    - автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
    - тестирование загруженных обновлений средствами программного обеспечения 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;
    - автоматическое развертывание по требованию специализированной системы защиты для виртуальных инфраструктур на базе Microsoft Hyper-V;
    - построение многоуровневой системы управления с возможностью настройки ролей 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 программного средства через сервер управления;
    - автоматическое распространение лицензии на клиентские компьютеры;
    - инвентаризация установленного программного обеспечения   
      и оборудования на компьютерах пользователей;
    - возможность подключения по RDP или штатными средствами   
      из консоли управления. Пользователю должен выводиться запрос   
      на разрешение дистанционного подключения;
    - наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
    - функция управления мобильными устройствами через сервер Exchange ActiveSync;
    - функция управления мобильными устройствами через сервер iOS MDM;
    - возможность отправки SMS-оповещений о заданных событиях;
    - централизованная установка приложений на управляемые мобильные устройства;
    - централизованная установка сертификатов на управляемые мобильные устройства;
    - поддержка функциональности управления шифрованием данных;
    - 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 как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и тд;
    - 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;
    - наличие веб-консоли управления приложением;
    - веб-консоль должна обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
    - наличие системы контроля возникновения вирусных эпидемий.
  1. Требования к обновлению антивирусных баз.

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

* + - регламентное обновление 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.
  1. 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   
       и руководство пользователя (администратора).
     + документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.
  2. Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

* + - Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Республики Беларусь круглосуточно без праздников   
      и выходных по телефону, электронной почте и через Интернет;
    - Web-сайт производителя антивирусного программного средства должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного программного средства, пополняемую базу знаний, а также форум пользователей программных продуктов.

1. **Права на компьютерную программу «Kaspersky Hybrid Cloud Security, Server for Virtualization», продление 10 пользователей (или узлов защиты), срок действия 12 месяцев.**
   1. Антивирусные средства защиты для виртуальных сред должны включать:
      * программные средства антивирусной защиты для виртуальных сред   
        с использованием агентов;
      * программные средства централизованного управления, мониторинга   
        и обновления;
      * обновляемые базы данных сигнатур вредоносных программ и атак;
      * эксплуатационную документацию на русском языке.
   2. Требования к программным средствам антивирусной защиты виртуальных сред c использованием агентов

Требования к гипервизору:

* + - Windows Server 2012 R2 с серверной ролью Hyper-V;
    - Windows Server 2016 с серверной ролью Hyper-V.
    - Windows Server 2019 с серверной ролью Hyper-V.

Требования к гостевой операционной системе гипервизора Hyper-V:

* + - Windows 7 Enterprise 32-bit/64-bit;
    - Windows 7 Professional SP1 32-bit/64-bit;
    - Windows 10;
    - Windows 11;
    - Windows Server 2008 R2 SP2;
    - Windows Server 2012 R2;
    - Windows Server 2016;
    - Windows Server 2019;
    - Windows Server 2022.

Программные средства антивирусной защиты виртуальных сред должны обеспечивать реализацию следующих функциональных возможностей:

* + - резидентный антивирусный мониторинг;
    - защита от программ-маскировщиков, программ автодозвона на платные сайты;
    - эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
    - вынесение антивирусного сканирования и других ресурсоемких задач   
      со всех гостевых машин на отдельную машину защиты;
    - автоматическое обнаружение и подключение к функционирующей машине защиты, в том числе находящейся на другом хосте, в случае недоступности основной машины защиты;
    - обеспечение непрерывности файловой защиты в период кратковременной недоступности машины защиты посредством журналирования всех файловых операций на защищаемой ВМ в период недоступности машины защиты, и выполнение автоматического сканирования всех изменений после восстановления доступа;
    - защита электронной корреспонденции от вредоносных программ   
      с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 — независимо от используемого почтового клиента;
    - защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных сайтов;
    - блокировка баннеров и всплывающих окон, загружаемых с Web-страниц;
    - распознавание и блокировка фишинг-сайтов;
    - проверка трафика ICQ и MSN, для обеспечения безопасности работы   
      с интернет-пейджерами;
    - защита от еще не известных вредоносных программ на основе анализа   
      их поведения;
    - возможность определения аномального поведения приложения   
      с помощью анализа последовательности действий этого приложения.
    - возможность совершить откат действий вредоносного программного обеспечения при лечении;
    - возможность ограничения привилегий исполняемых программ таких   
      как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы;
    - наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ;
    - 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;
    - наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме MD5, так и по заранее заданным категориям приложений, предоставляемым вендором, а также обеспечивать возможность исключения из правил для определенных пользователей из AD;
    - осуществление 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 AD;
    - осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки определенного типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из AD;
    - централизованные обновления с возможностью хранения части антивирусных баз на машине защиты;
    - запуск специальной задачи для обнаружения уязвимостей   
      в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
    - интеграция с системой обновления Windows Update для установки патчей, закрывающих обнаруженные уязвимости;
    - возможность удаленной установки и распространения компонентов антивирусного программного обеспечения на все защищаемые виртуальные машины без использования сторонних средств;
    - возможность проверки всех виртуальных машин по заранее заданному расписанию;
    - предотвращение повторного сканирования уже проверенных файлов;
    - наличие информации о проверенных файлах на машине защиты, позволяющей исключить повторную проверку одних и тех же файлов, находящихся на разных виртуальных машинах;
    - блокирование, обезвреживание и удаление вредоносного программного обеспечения, уведомление администраторов;
    - единая консоль управления для всех компонентов защиты;
    - консоль централизованного управления, единая для виртуальных сред   
      и физических рабочих станций;
    - предоставление подробной информации о событиях на виртуальных машинах и о выполнении задач;
    - возможность применять различные параметры безопасности   
      для отдельных групп виртуальных машин;
    - хранение резервных копий удаленных файлов;
    - поддержка технологий Hyper-V: Live migration, Cluster shared volumes, Dynamic memory, Live backup;
    - поддержка отката антивирусных баз;
    - поддержка схемы лицензирования как по числу защищаемых виртуальных машин, так и по количеству ядер CPU аппаратного обеспечения.

1. **Права на компьютерную программу «Kaspersky Embedded Systems Security», закупка 10 пользователей, срок действия 12 месяцев.**
   1. Антивирусные средства защиты для встроенных систем под управлением Microsoft Windows должны включать:
      * программные средства антивирусной защиты для рабочих станций и встроенных систем под управлением Windows;
      * программные средства централизованного управления, мониторинга   
        и обновления;
      * обновляемые базы данных сигнатур вредоносных программ и атак;
      * эксплуатационную документацию на русском языке.
   2. Требования к программным средствам антивирусной защиты рабочих станций и встроенных систем под управлением Windows.

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

* + - Microsoft Windows XP Professional SP2/SP3 и выше x86;
    - Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 и выше x86/x64;
    - Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
    - Microsoft Windows Embedded Standard 7 SP1 x86 / x64;
    - Microsoft Windows Embedded 8.0 Standard x64;
    - Microsoft Windows 10 Professional/Enterprise/IoT x86 / x64 1607-21H1;
    - Windows 10 IoT Enterprise LTSC 2016-2019 x86/x64;
    - Windows 11 21H2 Professional/Enterprise x64.

Программные средства антивирусной защиты для рабочих станций   
и встроенных систем под управлением Windows должны обеспечивать реализацию следующих функциональных возможностей:

* + - постоянная защита файлов, альтернативных потоков файловых систем (NTFS-streams), основных загрузочных записей и загрузочных секторов локальных жестких и съемных дисков;
    - контроль запуска программ с отслеживанием попытки запуска программ пользователями и возможностью регулирования запуска программ   
      на защищаемом устройстве;
    - контроль регистрации и использования внешних устройств с целью защиты устройства от угроз компьютерной безопасности, которые могут возникнуть во время файлового обмена с USB-подключаемым флеш-накопителем или внешними устройствами других типов;
    - настройки параметров и правил сетевого экрана операционной системы и блокировки любой возможности настройки параметров сетевого экрана извне;
    - обнаружение изменений в файлах из области мониторинга, указанной   
      в параметрах задачи и отображение этих изменений как нарушение безопасности на защищаемом устройстве;
    - контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows;
    - обновление баз и модулей программы с FTP- или HTTP-серверов обновлений;
    - запись событий информацию о параметрах функциональных компонентов программы, текущем состоянии задач, событиях, возникших за время их выполнения, а также о событиях, связанных   
      с управлением программным средством, и информацию, необходимую для диагностики сбоев в работе программы;
    - список исключений из области защиты или проверки компьютера;
    - защита памяти процессов от эксплуатации уязвимостей с помощью внедряемого в процессы Агента защиты.