

УТВЕРЖДАЮ:
Начальник управления
информационных технологий
АО «НЭСК»

Пилецкий О.В.

« ____ » _____ 2023г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на приобретение антивирусного программного обеспечения**

1. Заказчик – АО «НЭСК» (гор. Краснодар, пер. Переправный, д. 13).
2. Исполнитель договора на приобретение антивирусного программного обеспечения определяется по итогам проведения конкурсных процедур.
3. Период действия договора – до момента исполнения обязательств по договору.

4. Цель и основные требования:

4.1. Цель: обеспечение АО «НЭСК» российским антивирусным программным обеспечением, которое осуществляет комплексную многоуровневую защиту корпоративной сети от известных, неизвестных и сложных угроз.

4.2. Спецификация:

Заказчику требуется продление предоставления неисключительных прав на следующее программное обеспечение:

№ п.п.	Наименование	Характеристики	Количество, шт
1	Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 1000-1499 Node 1 year Renewal License	Обеспечение антивирусной защитой 1250 рабочих станций	1250
2	Kaspersky Security для почтовых серверов Russian Edition. 150-249 MailAddress 1 year Renewal License	Обеспечение антивирусной защитой 150 почтовых серверов	150

6. Общие требования

Средства антивирусной защиты для рабочих станций Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу В и Г не ниже второго класса защиты.

6.1 Антивирусная защита 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.

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 и фильтрации спама с помощью отдельного хоста
- Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange
- Программные средства централизованного управления, мониторинга и обновления.
- Обновляемые базы данных сигнатур вредоносных программ и атак.
- Эксплуатационную документацию на русском языке.

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

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

6.2 Требования к программным средствам антивирусной защиты для рабочих станций Windows.

Средства антивирусной защиты для рабочих станций Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу В и Г не ниже второго класса защиты.

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

- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows 10;

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

- возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью
- возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту.
- возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего.
- возможность читать информацию из записей аудита.
- ограничение доступа к чтению записей аудита.
- поиск, сортировка и упорядочение данных аудита.
- возможность уполномоченным пользователям (ролям) управлять параметрами средства антивирусной защиты, режимом выполнения функций безопасности средства антивирусной защиты;
- возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности, управлять установкой обновлений (актуализацией) антивирусных баз;
- поддержка определенных ролей их ассоциации с конкретными администраторами безопасности и пользователями.
- возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации.
- возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных.
- возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
- возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти,

удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов, удаления кода из файлов и системных областей носителей информации;

- возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы.
- отображение сигнала тревоги об обнаружении зараженных файлов
- возможность восстановления функциональных свойств зараженных объектов.
- возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса;
- Возможность контроля доступа к веб-ресурсам;
- Возможность контроля за запуском ПО на защищаемой рабочей станции или сервере.

6.3 Кроме того, программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

- антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализация действий активного заражения;
- анализ поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
- анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокирование действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- возможность совершить откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- возможность 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;

- возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени для получения вердикта по запускаемой программе или файлу;
- антивирусная проверка и лечение 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;
- фильтр почтовых вложений с возможностью переименования или удаления заданных типов файлов;
- проверка трафика, поступающего на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
- блокировка баннеров и всплывающих окон на загружаемых Web-страницах;
- распознавание и блокировка фишинговых и небезопасных сайтов;
- наличие 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;
- контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
- наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп). Компонент 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;
- 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;
- возможность записи в журнал событий о записи и/или удалении файлов на съемных дисках;
- осуществление контроля работы пользователя с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически

обновляемой производителем, а также типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;

- наличие механизмов защиты от атак типа BadUSB;
- запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- полnodисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;
- восстановления зашифрованного содержимого в случае сбоя загрузочного агента или файлов ОС, поддержка UEFI-систем;
- поддержка двухфакторной аутентификации при полnodисковом 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.
- 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;
- запуск задач по расписанию и/или сразу после запуска приложения;
- гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- возможность проверки целостности антивирусной программы;
- возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
- наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

- наличие защищенного хранилища для отчетов о работе антивируса;
- возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей.

6.4 Требования к программным средствам антивирусной защиты для файловых серверов Windows.

Средства антивирусной защиты для файловых серверов Windows должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты.

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

- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1;
- Microsoft Windows Server 2008 Standard / Enterprise x86 Edition SP2;
- Microsoft Windows Server 2008 Standard / Enterprise x64 Edition SP2;
- Microsoft Windows Small Business Server 2011 Essentials / Standard x64 Edition;
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition;
- Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition;
- Microsoft Windows MultiPoint Server 2012 x64 Edition;
- Microsoft Windows Server 2016 (без использования ReFS, Server Core, Server Nano и Cluster Mode);
- Microsoft Windows Server 2019 (без использования ReFS, Server Core, Server Nano и Cluster Mode).

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

- возможность идентификации и аутентификации администраторов безопасности до выполнения функций безопасности, связанных с управлением безопасностью
- возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту.
- возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего.
- возможность читать информацию из записей аудита.
- ограничение доступа к чтению записей аудита.
- поиск, сортировка и упорядочение данных аудита.
- возможность уполномоченным пользователям (ролям) управлять параметрами средства антивирусной защиты, режимом выполнения функций безопасности средства антивирусной защиты;

- возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности, управлять установкой обновлений (актуализацией) антивирусных баз;
- поддержка определенных ролей их ассоциации с конкретными администраторами безопасности и пользователями.
- возможность выполнять проверки с целью обнаружения зараженных объектов в файловых областях носителей информации, в оперативной памяти, в системных областях носителей информации, в файлах, в том числе исполняемых, упакованных различными средствами архивации.
- возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных.
- возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
- возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из оперативной памяти, удаления файлов, в которых обнаружены вредоносная составляющая, а также подозрительных файлов, возможность перемещения и изолирования зараженных объектов, удаления кода из файлов и системных областей носителей информации;
- возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы.
- отображение сигнала тревоги об обнаружении зараженных файлов
- возможность восстановления функциональных свойств зараженных объектов.
- возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса;
- возможность контроля за запуском ПО на защищаемой рабочей станции или сервере.

Кроме того, программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

- антивирусное сканирование в режиме реального времени и по запросу;
- антивирусное сканирование по команде пользователя или администратора и по расписанию;

- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- возможность приложения обратиться к локальным репутационным облачным сервисам в режиме реального времени для получения вердикта по запускаемой программе или файлу;
- 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 правил 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, LHA, JAR, ICE.
- 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;
- 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 SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, а также обеспечивать возможность исключения из правил для определенных пользователей из Active Directory;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

6.5 Требования к программным средствам антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows.

Средства антивирусной защиты серверов масштаба предприятия и терминальных серверов Windows должны быть сертифицированы в

соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты.

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

- Small Business Server 2008
- Windows MultiPoint Server 2011
- Windows Storage Server 2012, 2012 R2, 2016
- Windows Server 2008, 2008R2
- Windows Server 2012, 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Hyper-V Server

Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны функционировать на следующих типах терминальных серверов:

- Microsoft Remote Desktop Services на базе Windows 2008 Server;
- Microsoft Remote Desktop Services на базе Windows 2008 R2 Server;
- Microsoft Remote Desktop Services на базе Windows 2012 Server;
- Microsoft Remote Desktop Services на базе Windows 2012 Server R2;
- Microsoft Remote Desktop Services на базе Windows Server 2016;
- Microsoft Remote Desktop Services на базе Windows Server 2019;
- Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15;
- Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15.

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

- возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту;
- возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
- возможность читать информацию из записей аудита;
- ограничение доступа к чтению записей аудита;
- поиск, сортировка и упорядочение данных аудита;
- возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности;
- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;
- поддержка определенных ролей их ассоциации с конкретными администраторами безопасности и пользователями;

- возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных;
- возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
- возможность выполнять проверки с целью обнаружения зараженных объектов по команде и(или) в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, а также путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- возможность удаления (если технически возможно) файлов, в которых обнаружен вредоносный код, а также файлов, подозрительных на наличие вредоносного кода, перемещение и изолирование объектов воздействия;
- возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы;
- возможность отображение сигнала тревоги об обнаружении на рабочей станции администратора, в том числе до подтверждения его получения или до завершения сеанса;
- возможность восстановления функциональных свойств зараженных объектов;
- возможность получения и установки обновлений антивирусных баз без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения;
- возможность выполнять проверки с целью обнаружения атаки эксплойтов в памяти процессов, в контейнерах Windows Server 2016;
- возможность при обнаружении признаков атаки эксплойтов на защищаемый процесс завершать процесс, сообщать о факте дискредитации уязвимости в процессе.

Кроме того, программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

- антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: Серверов терминалов и 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, LHA, JAR, ICE;
- защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
- непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматическое запрещение выполнения тех из них, которые признаются опасными.
- Анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- Возможность проверки контейнеров Microsoft Windows.
- защита от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
- защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов. Перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления.
- наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп);
- компонент создания специальных правил должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
- компонент создания специальных правил должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должен иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
- осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
- осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем.;
- Информирование администратора о подключении внешних устройств.
- 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;
- Наличие механизмов автоматической генерации правил для контроля устройств и приложений;
- 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;

6.6. Требования к программным средствам антивирусной защиты и фильтрации спама с помощью отдельного хоста.

Средства антивирусной защиты и фильтрации спама с помощью отдельного хоста должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже четвертого класса защиты.

Программное средство антивирусной защиты и фильтрации спама должно обеспечивать реализацию следующих функциональных возможностей:

- поддержку определенных ролей для программного изделия и их ассоциации с конкретными администраторами безопасности, администраторами серверов и пользователями;
- возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности;

- возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности программного изделия;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ;
- получение и установка обновлений баз без применения средств автоматизации, в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения;
- возможность генерировать записи аудита для событий, подвергаемых аудиту;
- возможность чтения информации из записей аудита;
- возможность ассоциации событий аудита с идентификаторами субъектов;
- возможность ограничения доступа к чтению записей аудита;
- возможность поиска, сортировки, упорядочения данных аудита;
- возможность выполнения проверки с целью обнаружения зараженных объектов, в том числе и в режиме реального времени в файлах, полученных по каналам передачи данных;
- возможность выполнения проверки с целью обнаружения зараженных объектов по команде, в режиме динамического обнаружения в процессе выполнения операций доступа к объектам, путем запуска с необходимыми параметрами функционирования своего кода внешней программой;
- возможность выполнения проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами;
- возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из зараженных объектов;
- возможность выполнения проверок сообщений электронной почты на предмет наличия незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

Кроме того, программное средство антивирусной защиты должно обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

Программные средства антивирусной защиты и фильтрации спама должны поставляться в виде виртуального почтового шлюза с возможностью интеграции его в существующую почтовую структуру организации, а также в виде ISO инсталляционного образа.

Программные средства антивирусной защиты и фильтрации спама должны иметь возможность установки на виртуальные серверы, а так же непосредственно на физические серверы.

В состав виртуального почтового шлюза должны входить:

- Предустановленная ОС;
- Почтовый сервер;
- Антивирусная программа.

В процессе установки почтового шлюза из ISO образа должны устанавливаться:

- Операционная система;
- Почтовый сервер;
- Антивирусная программа.

Должна быть возможность установки почтового шлюза на следующие версии гипервизоров:

- VMware ESXi 5.5 Update 2;
- VMware ESXi 6.0;
- Microsoft Hyper-V Server 2012 R2.

Почтовый шлюз должен удовлетворять следующим минимальным требованиям:

- сетевой адаптер E1000;
- объем свободного места на диске – не менее 100 ГБ;
- не менее 4 ГБ оперативной памяти;
- один четырехъядерный процессор.

Должен быть предоставлен веб-интерфейс взаимодействия с почтовым шлюзом.

Веб-интерфейс должен быть протестирован на совместимость со следующими версиями браузеров:

- Mozilla Firefox версии 59 и выше.
- Internet Explorer версии 11 и выше.
- Google Chrome версии 65 и выше.

- Поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;

- Проверки входящий поток почтовых сообщений на наличие спама, потенциального спама, массовых рассылок (в том числе маркетинговые рассылки) удалять сообщения, помещать копии сообщений в хранилище;

- Управление анти-спам карантинном из веб-интерфейса;

- Детектирования вредоносных и фишинговых ссылок в теле письма;

- Наличие репутационных облачных сервисов;

- Возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку файлов, не отправляя данные за пределы организации;

- Наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки ранее неизвестных угроз;

- Обнаруживать, блокировать и лечить зараженные почтовые сообщения и зараженные вложения, удалять сообщения и вложения, помещать копии сообщений во временное хранилище;

- Обнаруживать и блокировать сообщения, содержащие макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять

сообщения или вложения, помещать копии сообщений во временное хранилище;

- Обнаруживать и блокировать сообщения, содержащие зашифрованные объекты, удалять сообщения или вложения, помещать копии сообщений во временное хранилище;
- Обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов (например, файлы формата ZIP, RAR, TGZ, 7z, QZIP), блокировать отдельные файлы внутри архивов;
- Выполнять контентную фильтрацию сообщений по имени, размеру и типу вложений, определять истинный формат и тип вложения, независимо от его расширения, удалять сообщения, содержащие вложения определенного формата или с определенным именем или сообщения, размер которых превышает допустимый, помещать копии сообщений во временное хранилище;
- Сохранять резервные копии сообщений во временное хранилище по результатам их обработки модулями защиты;
- Управление временным хранилищем из веб интерфейса;
- Сохранять сообщения из хранилища в файл и пересылать сообщения получателям
- Интеграции со службами каталогов Active Directory и Open LDAP;
- Возможность отправки ловушек и уведомлений по протоколу SNMP;
- Возможность работы по протоколу IPv6;
- Обрабатывать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей;
- Отправлять уведомления пользователям о результатах проверки их сообщений модулями программы;
- Уведомления должны содержать список последних сообщений в хранилище
- Настройки расписания отправки уведомлений;
- Обновления баз с использованием протоколов HTTP, HTTPS;
- Отправлять и получать сообщения по защищенному каналу TLS/SSL, осуществлять управление ключами шифрования;
- Осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM;
- Подписывать исходящие сообщения электронной почты с помощью технологии DKIM;
- Добавлять предупреждения о небезопасном вложении к входящим сообщениям;
- Просматривать журнал событий, аудита в веб интерфейсе программы и загружать его на жесткий диск;
- Обновлять систему через веб-интерфейс;
- Взаимодействие с службой технической поддержки через веб-интерфейс;

- Фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
- Проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
- Проверка IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF);
- Проверка с помощью сервиса SPAM URI Realtime Blocklists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
- Проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
- Выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка;
- Перенос в карантинный каталог зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы, а также файлы, в результате проверки которых произошла ошибка;
- Наличие общего и персонального карантина;
- Обработка почтового трафика в соответствии с правилами, заданными для групп отправителей и получателей;
- Организация дополнительной фильтрации почтового потока сообщений по именам и типам вложенных файлов и применение к отфильтрованным сообщениям отдельных правил обработки;
- Использование регулярных выражений при создании правил фильтрации;
- Наличие встроенных ролей администратора и специалиста поддержки;
- Возможность уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем заражённые и подозрительные объекты;
- Управление работой программы должно осуществляться как стандартными средствами операционной системы с помощью командной строки, так и через специальный веб-интерфейс, работающий на браузерах: Internet Explorer, Mozilla Firefox, Google Chrome;
- возможность добавления в сообщения X-заголовки X-MS-Exchange-Organization-SCL по результатам проверки на спам;
- возможность интеграции с SIEM-системами с использованием CEF-формата файлов;
- возможность добавлять метку Unicode_spoof к заголовку сообщения в случае обнаружения Юникод-спуфинга.
- Наличие гибкого инструментария для создания отчетов в формате PDF. Программные средства антивирусной защиты и фильтрации спама должны поставляться в виде виртуального почтового шлюза с возможностью интеграции его в существующую почтовую структуру организации, а также в виде ISO инсталляционного образа.

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

Средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу Б не ниже второго класса защиты. Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2012, 2012 R2
- Microsoft Windows Server 2008 R2
- Microsoft Windows® Small Business Server 2011 SP1 Standard;

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

- Microsoft Exchange Server 2010 SP3
- Microsoft Exchange Server 2013 SP1
- Microsoft Exchange Server 2016

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны обеспечивать реализацию следующих функциональных возможностей:

- Возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту.
- Возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего.
- Возможность читать информацию из записей аудита.
- Ограничение доступа к чтению записей аудита.
- Поиск, сортировка, упорядочение данных аудита.
- возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности программного изделия
- Возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности.
- Поддержка определенных ролей и их ассоциации с конкретными администраторами безопасности и пользователями.
- Возможность выполнять проверки с целью обнаружения зараженных объектов.
- Возможность выполнения проверок с целью обнаружения зараженных объектов в режиме реального времени в файлах, полученных по каналам передачи данных.
- Возможность выполнять проверки с целью обнаружения зараженных объектов сигнатурными и эвристическими методами.

- Возможность выполнять проверки с целью обнаружения зараженных объектов по команде. в режиме динамического обнаружения в процессе выполнения операций доступа к объектам.
- Возможность выполнять проверки с целью обнаружения зараженных объектов путем запуска с необходимыми параметрами функционирования своего кода средой функционирования.
- Возможность удаления (если удаление технически возможно) кода вредоносных компьютерных программ (вирусов) из зараженных объектов;
- Возможность отображения сигнала тревоги на АРМ администратора;
- возможность управления установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов);
- возможность получения и установки обновлений без применения средств автоматизации; в автоматизированном режиме с сетевого ресурса; автоматически через сетевые подключения;
- выполнение проверок сообщений электронной почты на предмет наличия незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

Кроме того, программные средства антивирусной защиты и фильтрации спама для почтовых серверов Microsoft Exchange должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

- совместимость с DAG в Microsoft Exchange;
- поддержка ролей MS Exchange 2010: Edge, Hub transport, Mailbox;
- поддержка ролей MS Exchange 2013: Mailbox, Edge Transport, Client Access Server (CAS);
- поддержка ролей MS Exchange 2016: Mailbox, Edge Transport;
- поддержка ролей MS Exchange 2019: Mailbox, Edge Transport;
- поиск и удаление по требованию всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
- поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в хранящихся на сервере Microsoft Exchange (в том числе в общих папках) сообщениях, включая вложения;
- наличие эвристических методов детектирования;
- проверка почтовых хранилищ и общих папок на сервере, в фоновом режиме для гарантированной обработки всех объектов с использованием самой актуальной версии антивирусных баз без заметного увеличения нагрузки на сервер;
- возможность лечить зараженные архивы;
- возможность выявления и удаления не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы,

программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях;

- возможность детектирования вредоносных и фишинговых ссылок в теле письма;
- наличие механизма распознавания вирусных эпидемий позволяющего своевременно (в том числе автоматически) предпринимать меры по усилению антивирусной защиты почтового сервера: при достижении заданного порога вирусной активности администратор сети получает уведомление по электронной почте;
- сохранение копий изменяемых сообщений в резервном хранилище, что позволяет восстановить важную информацию в случае некорректного лечения объекта;
- набор параметров поиска для удобства нахождения объекта в резервном хранилище;
- дополнительный уровень проверки с помощью репутационных облачных сервисов
- наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки ранее неизвестных угроз
- проверка различных параметров письма, таких как адреса отправителей и получателей, размер письма, а также поля заголовка сообщения;
- фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
- проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
- проверка IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF);
- проверка с помощью сервиса SPAM URI Realtime Block lists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
- использование контентной фильтрации (анализ содержимого самого письма, включая заголовки Subject и файлов вложений);
- возможность использовать роли пользователей/администраторов для разграничения доступа к настройке безопасности;
- возможность логирования / аудита изменения настроек безопасности различными пользователями системы;
- возможность получения отчётов и управления чёрными/белыми списками посредством PowerShell;
- использование контентной фильтрации (анализ содержимого самого письма, включая заголовки Subject и имён файлов);
- возможность фильтрации файлов Microsoft Office, содержащих макросы;

- возможность проверки и удаления исходящих сообщений, являющихся спамом или содержащих фишинговые и вредоносные ссылки;
- проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
- создание отчетов по работе системы защиты;
- возможность автоматической рассылки отчетов администраторам по расписанию;
- возможность обновления антивирусных баз как с сайтов производителя, так и с внутренних сетевых ресурсов организации;
- возможность фоновой проверки почтовых ящиков и общих папок с использованием Exchange Web Services;
- детальные отчеты в формате HTML;
- наличие возможности отправки отчётов и уведомлений на указанные адреса электронной почты;
- мониторинг работы программы с помощью System Center - Operations Manager;
- интеграция с Active Directory;
- управление серверами защиты с помощью MMC консоли;
- централизованный просмотра состояния защиты;
- возможность распределять роли администраторов системы.

6.7. Требования к программным средствам централизованного управления, мониторинга и обновления

Средства централизованного управления, мониторинга и обновления должны быть сертифицированы в соответствии с требованиями к средствам антивирусной защиты – приказ ФСТЭК от 20 марта 2012 г. №28 уполномоченным органом (ФСТЭК), по типу А не ниже второго класса защиты. Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10
- Windows Server 2008, 2008R2
- Windows Server 2012, 2012 R2
- Windows Server 2016

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

- Microsoft SQL Server® 2008 Express 32-разрядная;
- Microsoft SQL 2008 R2 Express 64-разрядная;
- Microsoft SQL 2012 Express 64-разрядная;
- Microsoft SQL 2014 Express 64-разрядная;

- Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная;
- Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная;
- Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная;
- Microsoft SQL Server 2012 (все редакции) 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft Azure SQL Database;
- MySQL 5.5 32-разрядная / 64-разрядная (не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5);
- MySQL Enterprise 5.5 32-разрядная / 64-разрядная;
- MySQL 5.6 32-разрядная / 64-разрядная;
- MySQL Enterprise 5.6 32-разрядная / 64-разрядная;
- MySQL 5.7 32-разрядная / 64-разрядная;
- MySQL Enterprise 5.7 32-разрядная / 64-разрядная.

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

- Возможность генерировать записи аудита для событий, потенциально подвергаемых аудиту.
- Возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего.
- Возможность читать информацию из записей аудита.
- Ограничение доступа к чтению записей аудита.
- Поиск, сортировка данных аудита.
- Возможность уполномоченным пользователям (ролям) управлять данными (административными данными), используемыми функциями безопасности.
- возможность администраторам безопасности управлять режимом выполнения функций безопасности
- возможность отображения сигнала тревоги на автоматизированное рабочее место (АРМ) администратора безопасности, указывающего на обнаружение вредоносных компьютерных программ (вирусов) на пользовательских автоматизированных рабочих местах;
- возможность идентифицировать автоматизированные рабочие места, генерирующие события аудита, вредоносные компьютерные программы (вирусы), которые были обнаружены, и действия, предпринятые средствами антивирусной защиты;
- возможность продолжать отображение сигнала тревоги на автоматизированном рабочем месте администратора безопасности, пока не будет получено подтверждение его получения или пока не будет завершен сеанс администратора безопасности;
- Возможность получения и установки обновлений антивирусных баз в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения.

- Возможность централизованной установки компонентов антивирусной защиты на серверы и рабочие станции вычислительной сети.
- возможность обработки зараженных объектов на АРМ и серверах вычислительной сети;
- возможность выполнения автоматизированного запуска системы защиты на АРМ и серверах вычислительной сети с заданными условиями поиска и режимами реагирования по расписанию; выполнение удаленного администрирования процессов обнаружения вредоносного объекта, обновления баз данных и компонентов системы защиты;
- возможность создания внутренних учетных записей для аутентификации пользователей.

Кроме того, программные средства централизованного управления, мониторинга и обновления должны обеспечивать реализацию следующих функциональных возможностей, не требующих сертификацию ФСТЭК:

- выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
- возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
- возможность 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 обнаруженных компьютеров 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 ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;

- возможность иерархии триггеров по которым происходит перераспределение;
- автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
- 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 ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
- 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;
- 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;
- 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;
- наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal);
- должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;

- возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС;
- возможность импортировать образ операционной системы из дистрибутивов (WIM)
- наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии;
- автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры
- 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 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 по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
- наличие преднастроенных стандартных отчетов о работе системы;
- экспорт отчетов в файлы форматов PDF и XML;
- централизованное управление объектами резервных хранилищ и карантинных по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
- создание внутренних учетных записей для аутентификации на сервере управления;
- создание резервной копии системы управления встроенными средствами системы управления;
- поддержка Windows Failover Clustering;
- поддержка интеграции с Windows сервисом Certificate Authority;
- наличие веб-консоли управления приложением;
- наличие портала самообслуживания пользователей;
- портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотра мобильных устройств, отправки команд

блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;

- наличие системы контроля возникновения вирусных эпидемий;
- возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF.
- возможность установки в облачной инфраструктуре Microsoft Azure;
- возможность интеграции по OpenAPI
- возможность управления антивирусной защитой с использованием WEB консоли

7. 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.

8. 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.

9. 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 Российской Федерации по телефону, электронной почте и через Интернет.
- Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.

10. Требования к сроку поставки программного обеспечения

АО «НЭСК», 350033, г. Краснодар, пер. Переправный, 13, офис 101.

Поставка неисключительных прав на программное обеспечение осуществляется в течение рабочих 5 дней с момента подписания договора.

11. Требования к Участнику-Исполнителю

Участник-Исполнитель должен соответствовать требованиям:

- не проведение процедуры ликвидации Правообладателя и отсутствие решения арбитражного суда о признании Правообладателя несостоятельным (банкротом) и об открытии конкурсного производства;
- не приостановление деятельности в порядке, предусмотренном Кодексом Российской Федерации об административных правонарушениях, на день подачи заявки на участие в конкурсе;
- отсутствие у Правообладателя недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты любого уровня или государственные внебюджетные фонды за прошедший календарный год, размер которой превышает двадцать пять процентов балансовой стоимости активов по данным бухгалтерской отчетности за последний завершенный отчетный период;
- отсутствие в реестре недобросовестных поставщиков (подрядчиков, исполнителей) сформированном в порядке, определенном Федеральным законом от 05.04.2013 № 44-ФЗ, информации о Правообладателе, в том числе информации об его учредителях, о членах коллегиального исполнительного органа, лице, исполняющем функции единоличного исполнительного органа Правообладателя;
- отсутствие в реестре недобросовестных поставщиков сформированном в порядке, действовавшем до 01 января 2014 года, информации о Правообладателе, в том числе информации об его учредителях, о членах коллегиального исполнительного органа, лице, исполняющем функции единоличного исполнительного органа Правообладателя;
- отсутствие у руководителя Правообладателя, членов его коллегиального исполнительного органа, главного бухгалтера Правообладателя судимости за преступления в сфере экономики, а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товаров, выполнением работы, оказанием услуги, являющихся объектом осуществляемой закупки, и административного наказания в виде дисквалификации.

11.1. Участник-Исполнитель гарантирует, что он обладает всеми законными основаниями передавать права на использование ПО (подтверждается предоставлением надлежаще заверенной копии лицензионного договора с Правообладателем).