## **РАЗДЕЛ II. ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Техническое задание**

**(Описание объекта закупки)**

***«Приобретение неисключительных (пользовательских) прав на лицензионное программное обеспечение сроком на 1 год»***

|  |  |  |
| --- | --- | --- |
| ***№ п/п*** | ***Наименование объекта закупки*** | ***Количество товаров, функциональные, технические  и качественные характеристики, эксплуатационные характеристики объекта закупки и иные показатели, связанные с определением соответствия поставляемого товара потребностям заказчика*** |
| 1 | Приобретение неисключительных (пользовательских) прав на лицензионное программное обеспечение сроком на 1 год | В соответствии с приложениями №1, №2  к техническому заданию (описание объекта закупки) |

***Перечень подразделений и количество пользователей в них*** указан в приложении №2 к техническому заданию (описание объекта закупки), являющегося неотъемлемой частью настоящей документации об электронном аукционе.

***Приложение № 1 к техническому заданию***

***(описание объекта закупки)***

**Количество товаров, функциональные, технические и качественные характеристики, эксплуатационные характеристики объекта закупки и иные показатели, связанные с определением соответствия поставляемого товара потребностям заказчика**

|  |  |  |
| --- | --- | --- |
| ***№***  ***п/п*** | ***Наименование*** | ***Кол-во, шт.*** |
| 1 | Неисключительное право на антивирусное программное обеспечение для защиты рабочих станций и файловых серверов, лицензия на 1 год | 1872 |
| 2 | Неисключительное право на антивирусное программное обеспечение для защиты почтовых шлюзов, лицензия на 1 год | 490 |
| 3 | Неисключительное право на антивирусное программное обеспечение для защиты от нежелательных массовых почтовых рассылок – спама, лицензия на 1 год. | 250 |

**Общие требования:**

Средства антивирусной защиты, предназначенные для развертывания в государственных организациях, должны обладать сертификатом уполномоченного органа (ФСТЭК) на соответствие требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» по уровню контроля не ниже 4 и требованиям технических условий.

В рамках всей организации используются единые антивирусные средства.

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.

Антивирусные средства должны включать в себя:

* программные средства антивирусной защиты рабочих станций и серверов;
* программные средства антивирусной защиты почтовых шлюзов;
* программные средства защиты пользователей от нежелательных массовых почтовых рассылок – спама;
* программные средства антивирусной защиты мобильных устройств (смартфонов);
* программные средства централизованного управления, мониторинга и обновления;
* обновляемые базы данных сигнатур вредоносных программ и атак;
* эксплуатационную документацию на русском языке.

**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 Professional / Enterprise x86 / x64;
* Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
* Microsoft Windows 10 Pro / Enterprise x86 / x64;
* Microsoft Windows Server 2012 R2 Standard х64;
* Microsoft Windows Server 2012 Standard / Foundation х64;
* Microsoft Small Business Server 2011 Standard х64;
* Microsoft Windows Server 2008 R2 Standard / Enterprise х64 SP1;
* Microsoft Windows Server 2008 Standard / Enterprise x86 / х64 SP2;

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

* Антивирусное сканирование в режиме реального времени и по запросу.
* Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.
* Антивирусное сканирование 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.
* Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу.
* 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.
* 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 механизмов защиты от атак типа BadUSB.
* 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 или 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.
* 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.

**Требования к программным средствам антивирусной защиты для рабочих станций Linux:**

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

* Red Hat® Enterprise Linux® 6.7 x86/x64
* Red Hat® Enterprise Linux® 6.8 x86/x64
* Red Hat® Enterprise Linux® 7.2 x64
* Red Hat® Enterprise Linux® 7.3 x64
* CentOS-6.7 x86/x64
* CentOS-6.8 x86/x64
* CentOS-7.2 x64
* CentOS-7.3 x64
* SUSE® Linux Enterprise Desktop 12 x64
* openSUSE® 42.2 x64
* Debian GNU/Linux 7.10 x86/x64
* Debian GNU/Linux 7.11 x86/x64
* Debian GNU/Linux 8.6 x86/x64
* Debian GNU/Linux 8.7 x86/x64
* Ubuntu 10.04 LTS x86/x64
* Ubuntu 12.04 LTS x86/x64
* Ubuntu Server 14.04 LTS x86/x64
* Ubuntu Server 16.04 LTS x86/x64
* Ubuntu Server 16.10 LTS x86/x64
* OracleLinux 7.3 x64

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

* Резидентный антивирусный мониторинг.
* Проверка ресурсов доступных по SMB/CIFS/NFS
* Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.
* Антивирусное сканирование по команде пользователя или администратора и по расписанию.
* Антивирусная проверку и лечение файлов в архивах.
* Запуск задач по расписанию и/или сразу после загрузки операционной системы.
* Помещение подозрительных и поврежденных объектов на карантин.
* Возможность экспортировать и сохранять отчеты в форматах HTML и CSV.
* Возможность перехвата и проверки файловых операций на уровне SAMBA.
* Гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
* Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу.
* Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность.
* Возможность управления через пользовательский графический интерфейс.
* Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

**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 Small Business Server 2011 Standard х64;
* Microsoft Windows Server 2008 Standard / Enterprise SP2 x86/x64;
* Microsoft Windows Server 2008 R2 Standard / Enterprise x64 SP1;
* Microsoft Windows Server 2012 Standard / Foundation х64;
* Microsoft Windows Server 2012 R2 Standard х64.
* Microsoft Windows Server 2016 х64.

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

* 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.
* Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, 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 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.

**Требования к программным средствам антивирусной защиты для файловых серверов Linux:**

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

* Red Hat® Enterprise Linux® 6.7 x86/x64
* Red Hat® Enterprise Linux® 6.8 x86/x64
* Red Hat® Enterprise Linux® 7.2 x64
* Red Hat® Enterprise Linux® 7.3 x64
* CentOS-6.7 x86/x64
* CentOS-6.8 x86/x64
* CentOS-7.2 x64
* CentOS-7.3 x64
* SUSE® Linux Enterprise Desktop 12 x64
* openSUSE® 42.2 x64
* Debian GNU/Linux 7.10 x86/x64
* Debian GNU/Linux 7.11 x86/x64
* Debian GNU/Linux 8.6 x86/x64
* Debian GNU/Linux 8.7 x86/x64
* Ubuntu 10.04 LTS x86/x64
* Ubuntu 12.04 LTS x86/x64
* Ubuntu Server 14.04 LTS x86/x64
* Ubuntu Server 16.04 LTS x86/x64
* Ubuntu Server 16.10 LTS x86/x64
* OracleLinux 7.3 x64

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

* Резидентный антивирусный мониторинг.
* Антивирусное сканирование по команде пользователя или администратора и по расписанию.
* Проверка ресурсов доступных по SMB / NFS.
* Антивирусная проверка и лечение файлов в архивах.
* Запуск задач по расписанию и/или сразу после загрузки операционной системы.
* Помещение подозрительных и поврежденных объектов на карантин.
* Формирование отчетов в форматах HTML, CSV, PDF и XLS.
* Возможность перехвата и проверки файловых операций на уровне SAMBA.
* Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность.
* Удаленно через веб-браузер управлять антивирусом и настраивать его.
* Централизованно управляться с помощью единой системы управления.

**Требования к программным средствам антивирусной защиты для файловых серверов масштаба предприятия и терминальных серверов Windows:**

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

* Microsoft Windows Server 2008 Standard/Enterprise/DataCenter/Core SP1 и выше x86/x64;
* Microsoft Windows Server 2008 R2 Core/ Standard/Enterprise/DataCenter SP1 и выше x64;
* Microsoft Windows Server 2012 Core/Standard/Essential/DataCenter/Foundation x64;
* Microsoft Windows Server 2012 R2 Core/Standard/Essential/DataCenter/Foundation x64;
* Microsoft Windows Server 2016 Core/Standard/Datacenter/Essentials x64;
* Microsoft Windows Storage Server 2008 R2 x64;
* Microsoft Windows Storage Server 2008 R2 SP2 Standard/Workgroup x64;
* Microsoft Windows Storage Server 2012 (все редакции) x64;
* Microsoft Windows Storage Server 2012 R2 (все редакции) x64;
* Microsoft Windows Storage Server 2016 x64;
* Microsoft Windows Hyper-V Server 2008 R2 SP1 x64;
* Microsoft Windows Hyper-V Server 2012 x64;
* Microsoft Windows Hyper-V Server 2012 R2 x64;
* Microsoft Windows Hyper-V Server 2016 x64.
* Терминальные серверы:
* Microsoft Remote Desktop Services на базе Windows Server 2008;
* Microsoft Remote Desktop Services на базе Windows Server 2012;
* Microsoft Remote Desktop Services на базе Windows Server 2012 R2;
* Microsoft Remote Desktop Services на базе Windows Server 2012;
* Citrix XenApp 6.0/6.5/7.0/7.5 – 7.9;
* Citrix XenDeskTop 7.0/7.1/7.5/7.9.

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 и принт-серверов; 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.
* Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу.
* 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.
* Возможность блокировки доступа удаленного компьютера к сетевым ресурсам сервера.
* Отслеживание попыток вредоносного шифрования файлов на общих сетевых папках сервера и блокирование компьютеров с которых идет такая активность.
* 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)
* Наличие локальной консоли управления. Возможность подключения к другим средствам защиты для серверов масштаба предприятия с помощью локальной консоли.
* 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).
* Поддержка технологий ReFS (Resilient file system) и CSV (Cluster Shared Volume).
* Централизованно управляться с помощью единой системы управления.

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

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

* Microsoft Windows Server 2016;
* Microsoft Windows Server 2012 R2 Standard / Datacenter;
* Microsoft Windows Server 2012 Standard / Datacenter;
* Microsoft Windows Small Business Server 2011 SP1 Standard;
* Microsoft Windows Server 2008 R2 SP1 Standard / Enterprise / Datacenter.

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

* Microsoft Exchange Server 2010 SP3
* Microsoft Exchange Server 2013 SP1
* Microsoft Exchange Server 2016
* Программные средства антивирусной защиты для серверов Microsoft Exchange должны функционировать с серверами баз данных следующих версий:
* Microsoft SQL Server 2012
* Microsoft SQL Server 2014
* Microsoft SQL Server 2016

Консоль управления программными средствами антивирусной защиты для серверов Microsoft Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

* Microsoft Windows 10;
* Microsoft Windows 8.1;
* Microsoft Windows 8;
* Microsoft Windows 7 SP1 Professional /Enterprise / Ultimate;
* Microsoft Windows Server 2016;
* Microsoft Windows Server 2012 R2 Standard / Datacenter;
* Microsoft Windows Server 2012 Standard / Datacenter;
* Microsoft Windows Small Business Server 2011 SP1 Standard;
* Microsoft Windows Server 2008 R2 SP1 Standard / Enterprise / Datacenter.

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

* 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.
* 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.
* 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. Широкий 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 заголовок 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 посредствам PowerShell.
* Использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и файлов вложений).
* 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.
* Возможность управления всеми серверами защиты с помощью одной MMC консоли.

**Требования к программным средствам антивирусной защиты и фильтрации спама для Linux почтовых серверов:**

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

* Red Hat Enterprise Linux 6.6 Server x86/x64
* Red Hat Enterprise Linux 7.0 Server x64
* CentOS 6.6 x86/x64
* CentOS 7 x64
* SUSE Linux Enterprise Server 11 SP3 x86/x64
* SUSE Linux Enterprise Server 12 x64
* Ubuntu Server 12.04.4 LTS x86/x64
* Ubuntu Server 14.04 LTS x86/x64
* Debian GNU/Linux 6.0.10 x86/x64
* Debian GNU/Linux 7.7 x86/x64
* FreeBSD 8.3 x86/x64
* FreeBSD 9.3 x86/x64
* FreeBSD 10.1 x86/x64

Программные средства антивирусной антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать совместно с почтовыми системами следующих версий:

* exim-4.71 и выше
* postfix-2.5 и выше
* qmail-1.03 и выше
* sendmail-8.14 и выше

Программные средства антивирусной защиты и фильтрации спама должны иметь возможность поставки в виде интегрированного решения, как образ виртуальной машины для развертывания на гипервизорах:

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

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

* Использование средства антивирусной защиты и фильтрации спама с любой имеющейся почтовой системой;
* Проверка IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF); Поддержка технологий DKIM/DMARC;
* 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;
* Возможность детектирования вредоносных и фишинговых ссылок в теле письма;
* Наличие эвристических методов детектирования;
* Использования репутационных облачных сервисов;
* Проверка на наличие спама входящий поток почтовых сообщений;
* Наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки ранее неизвестных угроз;
* Контентная фильтрация почтовых сообщений по имени, типу и размеру вложений;
* Интеграция со службами каталогов Active Directory и Open LDAP;
* Возможность отправления ловушек и уведомлений по протоколу SNMP;
* Возможность работы по протоколу IPv6;
* Фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
* Проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
* Проверка с помощью сервиса SPAM URI Realtime Blocklists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
* Проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
* Выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка;
* Перенос в 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;
* Возможность создания персональных черного и белого списков;
* Осуществление по запросу антивирусной проверки объектов на файловой системе сервера;
* 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;
* Возможность работы через интерфейс Amavis;
* Управление работой программы должно осуществлять как стандартными средствами операционной системы с помощью командной строки, так и через специальный веб-интерфейс, работающий на браузерах: Internet Explorer, Mozilla Firefox, Google Chrome;
* Управление всеми функциями с помощью веб-интерфейса;
* 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;
* Наличие гибкого инструментария для создания отчетов в формате PDF.

**Требования к программным средствам для защиты от нежелательных почтовых рассылок – спама:**

Программные средства для почтовых шлюзов под управлением семейства ОС Linux, осуществляющие фильтрацию электронной почты от нежелательных массовых рассылок – спама обеспечивают защиту почтовых систем, функционирующих под управлением следующих 32-битных ОС:

* RedHat Linux 9.0;
* Fedora Core 3;
* RedHat Enterprise Linux Advanced Server 3;
* SuSe Linux Enterprise Server 9.0;
* SuSe Linux Professional 9.2;
* Mandrake Linux version 10.1;
* Debian GNU/Linux version 3.1r0;
* FreeBSD version 5.4;
* FreeBSD version 6.2.

И следующих версий почтовых систем:

* Sendmail 8.13.5 с поддержкой Milter API;
* Postfix 2.2.2;
* Qmail 1.03;
* Exim 4.50;
* Communigate Pro 4.3.7.

Программные средства для почтовых шлюзов под управлением семейства ОС Linux, осуществляющие фильтрацию электронной почты от нежелательных массовых рассылок – спама, обеспечивают реализацию следующих функциональных возможностей:

* проверку различных параметров письма, таких как адреса отправителей и получателей, размер письма, а также поля заголовка сообщения;
* проверку адреса отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
* проверку наличия IP-адреса отправителя в списках DNS-based real time black hole list (DNSBL);
* проверку IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF);
* проверку с помощью сервиса SPAM URI Realtime Blocklists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
* использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и файлов вложений);
* проверку графических вложений на совпадение с известными сигнатурами спам-сообщений.

**Требования к программным средствам антивирусной защиты смартфонов:**

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

* Android 4.1 – 7.1.1;
* Apple iOS 9.0 – 10.3;
* Windows Phone 8.1, 10 Mobile.
* 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 расписанию.
* 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.
* Базовая поддержка Android for Work.
* 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 так же 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.
* Программные средства для антивирусной защиты смартфонов для ОС Windows Phone должны обеспечивать следующую функциональность:
* Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты.
* Возможность определения местоположения устройства.

**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 SP1 x86 / x64;
* Microsoft Windows 8 Professional / Enterprise x86 / x64;
* Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
* Microsoft Windows 10 Professional/Enterprise/Education x86 / x64;
* Microsoft Windows 10 RS1 x86 / x64;
* Microsoft Windows 10 RS2 x86 / x64;
* Microsoft Windows Server 2008 Foundation/Standard/Enterprise/Datacenter SP1 x86 / x64;
* Microsoft Windows Server 2008;
* Microsoft Windows Server 2008 SP1 x86 / x64;
* Microsoft Windows Server 2008 R2 Core/Foundation/Standard/Enterprise/Datacenter x64;
* Microsoft Windows Server 2008 R2 Core/Foundation/Standard/Enterprise/Datacenter SP1 x64;
* Microsoft Windows Server 2012 Core/Foundation/Standard/Enterprise/Datacenter x64;
* Microsoft Windows Server 2012 R2 Core/Essentials/Foundation/Standard/Enterprise/Datacenter x64;
* Microsoft Windows Small Business Server 2008 Standard/Premium x64;
* Microsoft Windows Small Business Server 2011 Essentials/Premium/Standard x64.

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

* Microsoft SQL Express 2008/2008R2/2012/2014;
* Microsoft SQL Server 2008/2008R2/2012/2014/2016;
* Microsoft Azure SQL Database;
* MySQL 5.5, 5.6, 5.7 x86/x64;
* MySQL Enterprise 5.5, 5.6, 5.7 x86/x64.
* Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий:
* VMware Workstation 9.x, Workstation 10.x, 12x Pro;
* VMware vSphere 5.5, 6;
* Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 20012 R2;
* Microsoft VirtualPC 2007(6.0.156.0);
* Parallels Desktop 7,11;
* Citrix XenServer 6.1, 6.2, 6.5, 7;
* Oracle VM VirtualBox 4.0.4-70112.

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 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 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 их работе.
* 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 УЗ, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности. Должна быть реализована возможность поддержки иерархии таких триггеров.
* Автоматизированный поиск 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.
* Автоматическое развертывание по требованию специализированной системы защиты для виртуальных инфраструктур на базе VMware ESXi, Microsoft Hyper-V, Citrix XenServer .
* 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 ПО через сервер управления.
* Автоматическое распространение лицензии на клиентские компьютеры.
* Инвентаризация установленного ПО и оборудования на компьютерах пользователей.
* Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них.
* Функция управления мобильными устройствами через сервер Exchange ActiveSync.
* 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.
* 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 т.д.
* Наличие преднастроенных стандартных отчетов о работе системы.
* Экспорт отчетов в файлы форматов PDF и XML.
* Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение.
* Создание внутренних учетных записей для аутентификации на сервере управления.
* Создание резервной копии системы управления встроенными средствами системы управления.
* Поддержка Windows Failover Clustering.
* Поддержка интеграции с Windows сервисом Certificate Authority.
* Наличие веб-консоли управления приложением.
* Наличие портала самообслуживания пользователей. Портал самообслуживания должен обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя.
* Наличие системы контроля возникновения вирусных эпидемий.

**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.

**Требования к эксплуатационной документации**

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

* Руководство пользователя (администратора).

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

**Требования к документам для сертифицированной версии**

Поставляемый программный продукт должен включать в себя пакет документов для сертифицированной версии:

- верифицированный дистрибутив сертифицированного программного обеспечения (на физическом носителе);

- руководство по настройке (в электронном виде);

- формуляр на сертифицированное программное обеспечение, промаркированный специальными защитными знаками соответствия ФСТЭК России;

- копия Сертификата ФСТЭК России на программное обеспечение, заверенная печатью Заявителя;

- абонемент на сертификационную поддержку программного обеспечения (должен действовать в течение всего срока действия Сертификата ФСТЭК).

**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 АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов.

Антивирусные средства будут установлены на ПК структурных подразделений Администрации, приведенных в Таблице № 1

***Приложение № 2 к техническому заданию***

***(описание объекта закупки)***

***Таблица № 1***

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование подразделения** | **Количество пользователей** |
| **Антивирусное программное обеспечение для защиты рабочих станций и файловых серверов** | | |
| 1 | МКУ «Центр информационных технологий» городского округа город Уфа Республики Башкортостан | 62 |
| 2 | Администрация городского округа город Уфа Республики Башкортостан | 370 |
| 3 | Администрация Демского района округа город Уфа Республики Башкортостан | 70 |
| 4 | Администрация Калининского района округа город Уфа Республики Башкортостан | 100 |
| 5 | Администрация Кировского района округа город Уфа Республики Башкортостан | 90 |
| 6 | Администрация Ленинского района округа город Уфа Республики Башкортостан | 75 |
| 7 | Администрация Октябрьского района округа город Уфа Республики Башкортостан | 95 |
| 8 | Администрация Орджоникидзевского района округа город Уфа Республики Башкортостан | 110 |
| 9 | Администрация Советского района округа город Уфа Республики Башкортостан | 80 |
| 10 | Главное управление архитектуры и градостроительству Администрации округа город Уфа Республики Башкортостан | 120 |
| 11 | Управление по опеке и попечительству Администрации округа город Уфа Республики Башкортостан | 36 |
| 12 | Управление образования Администрации округа город Уфа Республики Башкортостан | 100 |
| 13 | Управление по культуре и искусству Администрации округа город Уфа Республики Башкортостан | 33 |
| 14 | Управление земельных и имущественных отношений Администрации округа город Уфа Республики Башкортостан | 288 |
| 15 | Управление коммунального хозяйства и благоустройства Администрации округа город Уфа Республики Башкортостан | 60 |
| 16 | Управление по физкультуре и спорту Администрации округа город Уфа Республики Башкортостан | 30 |
| 17 | Комитет по делам молодежи Администрации округа город Уфа Республики Башкортостан | 30 |
| 18 | Финансовое управление Администрации округа город Уфа Республики Башкортостан | 80 |
| 19 | Управление по строительству, ремонту дорог и искусственных сооружений Администрации округа город Уфа Республики Башкортостан | 43 |
| **ИТОГО** | | **1872** |
| **Антивирусное программное обеспечение для защиты почтовых шлюзов** | | |
| 1 | Администрация городского округа город Уфа Республики Башкортостан | 350 |
| 2 | Главное управление архитектуры и градостроительству Администрации округа город Уфа Республики Башкортостан | 140 |
| **ИТОГО** | | **490** |
| **Антивирусное программное обеспечение для защиты от нежелательных массовых почтовых рассылок** | | |
| 1 | Администрация городского округа город Уфа Республики Башкортостан | 250 |