АКЦИОНЕРНОЕ ОБЩЕСТВО
«БАШКИРСКАЯ СОДОВАЯ КОМПАНИЯ»

УТВЕРЖДАЮ

Техническое задание на закупку
Неисключительных прав (лицензий) на использование программного обеспечения антивирусной защиты АРМ

1. **Предмет закупки –** Предметом закупки является предоставление (передача) на условиях простой (неисключительной) лицензии права на использование программного обеспечения (далее по тексту ПО), включая право на воспроизведение указанного программного обеспечения, ограниченное правом инсталляции, копирования и запуска программного обеспечения в соответствии с документацией (соглашением) правообладателя, сопровождающей передачу прав пользования и устанавливающей правила использования программного обеспечения на территории Российской Федерации

2. **Общие требования**

Антивирусные средства должны включать:

№№	Наименование	Кол.
1	Неисключительное право на программное обеспечение Антивирус Касперского Kaspersky Endpoint Security для бизнеса - Стандартный, лицензия на 1 год, продление	2800

	для win7,8,10, Linux	
2	Неисключительное право на программное обеспечение Антивирус Касперского Kaspersky Endpoint Security для - банкоматов и точек мгновенной оплаты, лицензия на 1 год, продление для winxp	700
3	Неисключительное право на программное обеспечение Антивирус Касперского Kaspersky Endpoint Security для почтовых серверов лицензия на 1 год, продление	2100

- программные средства централизованного управления, мониторинга и обновления;
- обновляемые базы данных сигнатур вредоносных программ и атак сроком на 1 год;
- эксплуатационную документацию на русском языке.

Программное обеспечение антивирусной защиты должно быть включено в единый реестр отечественного программного обеспечения Минкомсвязи РФ.

Все поставляемые решения средств антивирусной защиты должны иметь единую консоль управления, мониторинга и обновлений.

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

3. Требования к программным средствам антивирусной защиты для рабочих станций

3.1. Требования к защите рабочих станций на базе Windows 7 и выше.

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

- Windows 7 Professional (32 / 64-разрядная);
- Windows 8 Professional (32 / 64-разрядная);
- Windows 8.1 Professional (32 / 64-разрядная);
- Windows 10 Pro (32 / 64-разрядная).
- ОС Linux

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

- антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализации действий активного заражения;
- анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- необходимость защиты от локальной атаки шифровальщика на пк пользователя, с возможностью восстановления повреждённых пользовательских данных;
- 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;
- антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
- фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
- проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
- блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
- распознавания и блокировку фишинговых и небезопасных сайтов;
- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;

- защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
- контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
- создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (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;
- записи в журнал событий о записи и/или удалении файлов на съемных дисках;
- назначение приоритета для правил доступа к устройствам с файловой системой;
- контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
- запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
- установки только выбранных компонентов программного средства антивирусной защиты;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- запуска 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;
- проверки целостности антивирусной программы;
- добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
- импорта и экспорта списков правил и исключений в XML-формат;
- наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
- наличие защищенного хранилища для отчетов о работе антивируса;
- включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
- наличие поддержки Antimalware Scan Interface (AMSI);
- защитить паролем восстановление объектов из резервного хранилища;
- ограничения сетевого трафика в том случае, если подключение к интернету является лимитным.
- необходимость поддержки облачных сетей вендора для предлагаемого антивирусного решения и повышения эффективности работы компонентов защиты.

3.2. Требования к защите рабочих станций на базе Windows XP.

Срок поддержки программных средств антивирусной защиты в течение одного года. Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:

- Windows XP Professional (32 / 64-разрядная);

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

- антивирусное сканирования в режиме реального времени;
- антивирусное сканирование по расписанию, планировщик задач, проверка задач, созданных в системном планировщике, выполняемые в рамках задач проверки по требованию с включённой областью проверки;
- ускорение процесса сканирования за счёт пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- автоматическое сканирование подключаемых устройств;

- эвристический анализ, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
- защита от сетевых атак с анализом сетевого трафика на наличие признаков сетевых атак;
- обнаружение подозрительной подписки в пространстве инструментария управления windows с последующим их удалением;
- управление антивирусным решением с помощью веб-консоли;
- возможность включения запуска задач проверки важных областей по обнаружении признаков активного заражения;
- возможность создания списков исключений, доверенных программ и их процессов;
- необходимость сбора информации контрольных сумм заражённых объектов в отчётности;
- возможность создания правил запуска программ на основе информации о заблокированных запусках процессов программ;
- управление подключениями дополнительного оборудования (сетевые карты, модемы и т.д.) с возможностью использования правил запрета;
- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила;
- проверки целостности антивирусной программы.

4. Требования к программным средствам антивирусной защиты для серверов масштаба предприятия, терминальных серверов Windows

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

- Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная);
- Windows Server 2008 R2 Standard / Enterprise Service Pack 1 (64-разрядная);
- Windows Server 2012 (64-разрядная);
- Windows Server 2012 R2 (64-разрядная);
- Windows Server 2016 (64-разрядная);
- Windows Server 2019 (64-разрядная).

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

- антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;

- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализации действий активного заражения;
- анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- необходимость защиты от локальной атаки шифровальщика на пк пользователя, с возможностью восстановления повреждённых данных;
- антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
- запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
- установки только выбранных компонентов программного средства антивирусной защиты;
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
- запуск задач по расписанию и/или сразу после загрузки операционной системы;
- гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
- ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- проверки целостности антивирусной программы;

- 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;
- включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
- защитить паролем восстановление объектов из резервного хранилища.
- импорта и экспорта списков правил и исключений в XML-формат;
- ограничения сетевого трафика в том случае, если подключение к интернету является лимитным.

5. Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Windows XP Professional (32 / 64-разрядная);
- Microsoft Windows 10 32-разрядная / 64-разрядная;
- Microsoft Windows 10 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;
- Microsoft Windows 7 Professional 32-разрядная / 64-разрядная;
- Windows Server 2019 Standard 64-разрядная;
- Microsoft Windows Server 2019 Datacenter 64-разрядная;
- Microsoft Windows Server 2016 Server Standard 64-разрядная;
- Microsoft Windows Server 2016 Server Datacenter 64-разрядная;
- Microsoft Windows Server 2016 Datacenter (LTSB) 64-разрядная;
- Microsoft Windows Server 2012 R2 Standard 64-разрядная;
- Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2012 Standard 64-разрядная;
- Microsoft Windows Server 2012 Datacenter 64-разрядная;

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

- выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
- чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;

- настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
- автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;
- централизованные установка, обновление и удаление программных средств антивирусной защиты;
- централизованная настройка, администрирование;
- просмотр отчетов и статистической информации по работе средств защиты;
- централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
- сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
- наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
- указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
- иерархии триггеров, по которым происходит перераспределение;
- тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
- доставка обновлений на рабочие места пользователей сразу после их получения;
- построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
- создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
- обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
- 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;
- построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
- наличие преднастроенных стандартных отчетов о работе системы;
- экспорт отчетов в файлы форматов PDF и XML;
- централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
- создание внутренних учетных записей для аутентификации на сервере управления;
- создание резервной копии системы управления встроенными средствами системы управления;
- поддержка интеграции с Windows сервисом Certificate Authority;
- управления антивирусной защитой с использованием WEB консоли, так и программноустанавливаемой;
- двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
- использования дополнительной аутентификация после изменения параметров учетной записи пользователя.
- централизованное управление мобильными устройствами и полнофункциональной защитой на базе ОС Android, iOS.

6. 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.

7. 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.

8. 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 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.

9. Условия поставки: электронная поставка.