ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 531252
способом Открытый тендер на понижение

Лот № (3-1 У, 1874058) Услуги по предоставлению лицензий на право использования программного обеспечения

Заказчик: Товарищество с ограниченной ответственностью "Energy Solutions Center "
Организатор: Товарищество с ограниченной ответственностью "Energy Solutions Center "

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	3-1 У
Наименование и краткая характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения, Услуги по предоставлению лицензий на право использования программного обеспечения
Дополнительная характеристика	Услуги на приобретение и внедрение лицензий технической поддержки системы контроля автоматизированных рабочих мест и серверов (Программное обеспечение по антивирусной защите)
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Нур-Султан, район "Есиль", , проспект Кабанбай батыра, дом №15А, Блок Б, Бизнес-центр «Q»
Условия поставки	-
Срок поставки	С даты подписания договора в течение 30 календарных дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

1. Предмет закупки: Услуги по предоставлению лицензий на право использования программного обеспечения (Программное обеспечение по антивирусной защите).

2. Требования к системе контроля автоматизированных рабочих мест и серверов.
2.1. Общие требования к функциональности системы.
2.1.1. Система должна включать:
Программные средства антивирусной защиты для рабочих станций Windows;
Программные средства антивирусной защиты для рабочих станций Linux;
Программные средства антивирусной защиты для серверов семейства Windows Server;
Программные средства антивирусной защиты для серверов семейства Unix/Linux;
Программные средства антивирусной защиты и фильтрации спама для почтовых серверов;
Программные средства антивирусной защиты для виртуальных серверов;
Программные средства централизованного управления, мониторинга и обновления;
Обновляемые базы данных сигнатур вредоносных программ и атак;
Эксплуатационную документацию на русском языке.
2.1.2. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой и программным интерфейсом на русском языке.
2.1.3. Все антивирусные средства должны быть от одного Производителя программного обеспечения.
2.2. Требования к программным средствам антивирусной защиты для рабочих станций Windows.
2.2.1. 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 Edition;
Microsoft Windows 7 Professional / Enterprise / Ultimate x86/x64 Edition SP1;
Microsoft Windows 8 Professional / Enterprise x86/x64 Edition;
Microsoft Windows 8.1 Professional / Enterprise x86/x64 Edition;
Microsoft Windows 10 Pro / Enterprise x86/x64 Edition и т.д.
2.2.2. Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:
Возможность генерировать записи аудита для событий потенциально подвергаемых аудиту;
Возможность ассоциации каждого события аудита с идентификатором его инициировавшего субъекта;
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 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;
Возможность выполнять проверки с целью обнаружения зараженных объектов 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;
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 отображения сигнала тревоги на рабочей станции пользователя или администратора безопасности, 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;
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;
Интеграция с локальным репутационным облаком, позволяющая приложению в режиме реального времени получать вердикт по запускаемой программе или файлу;
Защита электронной корреспонденции от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI (независимо от используемого почтового клиента);
Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, HTTPS, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных сайтов;
Блокировка баннеров и всплывающих окон, загружаемых с web-страниц;
Распознавание и блокировка фишинг-сайтов;
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;
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;
Полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single-Sign-On. Обязательно наличие инструментов восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС. Должна быть реализована поддержка UEFI-систем;
Поддержка двухфакторной аутентификации при полнодисковом 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;
Шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
Возможность экспортировать и сохранять отчеты в форматах HTML, CSV, PDF;
Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
2.3. Требования к программным средствам антивирусной защиты для рабочих станций Linux.
2.3.1. Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
Red Hat Enterprise Linux 5.8 Desktop x32/x64;
Red Hat Enterprise Linux 6.2 Desktop x32/x64;
SUSE Linux Enterprise Desktop 10 SP4 x32/x64;
SUSE Linux Enterprise Desktop 11 SP2 x32/x64;
Debian GNU/Linux 8 x32/x64;
Debian GNU/Linux 9 x32/x64;
Ubuntu Desktop 10.04 LTS x32/x64;
Ubuntu Desktop 12.04 LTS x32/x64;
Ubuntu Desktop 14.04 LTS x32/x64;
Ubuntu Desktop 16.04 LTS x32/x64;
Ubuntu Desktop 18.04 LTS x32/x64;
Ubuntu Desktop 19.04 LTS x32/x64 и т.д.
2.3.2. Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:
Обнаружение вредоносных программ и зараженных объектов;
Осуществлять защиту в режиме реального времени (осуществлять проверку файлов при обращении к ним со стороны ОС);
Обеспечивать возможность перехвата файловых операций на уровне SAMBA;
Обеспечивать возможность просмотра отчетов о работе программного изделия через командную строку и сохранение их в файл;
Осуществлять обновления баз антивируса из заданного источника;
Резидентный антивирусный мониторинг;
Проверка ресурсов доступных по SMB / 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 в 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;
Интеграция с локальным репутационным облаком, позволяющая приложению в режиме реального времени получать вердикт 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.
2.4. Требования к программным средствам антивирусной защиты для рабочих станций MacOS.
2.4.1. Программные средства антивирусной защиты для рабочих станций MacOS должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
Mac OS X 10.9 (Mavericks);
Mac OS X 10.8 (Mountain Lion);
Mac OS X 10.7 (Lion);
Mac OS X 10.6 (Snow Leopard);
Mac OS X 10.5 (Leopard);
Mac OS X 10.4 (Tiger) и т.д.
2.4.2. Программные средства антивирусной защиты для рабочих станций MacOS 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 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 и(или) 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 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 блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций или сервера, на которых обнаружены зараженные файлы;
Возможность отображения сигнала тревоги на рабочей станции пользователя или администратора безопасности, 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;
Резидентный антивирусный мониторинг;
Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
Антивирусное сканирование по команде пользователя или администратора и по расписанию;
Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
Интеграция с локальным репутационным облаком, позволяющая приложению в режиме реального времени получать вердикт по запускаемой программе или файлу;
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;
Блокировка вредоносных и фишинговых сайтов на основе вердиктов локальных репутационных облачных сервисов производителя антивирусных средств защиты;
Защита веб-трафика – проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, HTTPS;
Автоматическое обновление антивирусных баз по расписанию;
Возможность управления через пользовательский графический интерфейс;
Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
2.5. Требования к программным средствам антивирусной защиты для серверов семейства Windows.
2.5.1. Программные средства антивирусной защиты для серверов семейства Windows должны функционировать на серверах, работающих под управлением операционных систем следующих версий:
Microsoft Windows Server 2003 Standard x86/ x64 Edition SP2;
Microsoft Windows Server 2003 R2 Standard / Enterprise x86 Edition SP2;
Microsoft Windows Server 2003 R2 Standard x64 Edition SP2;
Microsoft Windows Server 2008 Standard / Enterprise x86/x64 Edition SP2;
Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition;
Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1;
Microsoft Windows Server 2012 Standard / Datacenter x64;
Microsoft Windows Server 2012 R2 Standard / Datacenter x64;
Microsoft Windows Server 2016 Standard / Datacenter x64;
Microsoft Windows Server 2019 Standard / Datacenter x64 и т.д.
2.5.2. Программные средства антивирусной защиты для серверов семейства 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 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;
Возможность выполнять проверки с целью обнаружения зараженных объектов 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;
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 отображения сигнала тревоги на рабочей станции пользователя или администратора безопасности, 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;
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;
Интеграция с локальным репутационным облаком, позволяющая приложению в режиме реального времени получать вердикт 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;
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.
2.6. Требования к программным средствам антивирусной защиты для серверов семейства Unix/Linux.
2.6.1. Программные средства антивирусной защиты для серверов семейства Unix/Linux должны функционировать на серверах, работающих под управлением операционных систем следующих версий:
Red Hat Enterprise Linux Server 6 x32/x64;
Red Hat Enterprise Linux Server 7 x64;
CentOS 6 x32/x64;
CentOS 7 x64;
Sangoma Linux 7;
SUSE Linux Enterprise Server 11 SP3 x32/x64;
SUSE Linux Enterprise Server 12 x64;
Ubuntu Server 12.04 LTS x32/x64;
Ubuntu Server 14.04 LTS x32/x64;
Ubuntu Server 16.04 LTS x32/x64;
Ubuntu Server 18.04 LTS x32/x64;
Debian GNU/Linux 7 x32/x64;
Debian GNU/Linux 8 x32/x64;

Debian GNU/Linux 9 x32/x64;
FreeBSD 8;
FreeBSD 9;
FreeBSD 10;
Astra Linux 1.4 x64;
Astra Linux 1.5 x64 и т.д.

2.6.2. Программные средства антивирусной защиты для файловых серверов Linux 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;
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 администраторами сервера;
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 и(или) 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 внешней программой;
Возможность удаления (если технически возможно) файлов, в которых обнаружена вредоносная составляющая, а также подозрительных файлов, перемещение и изолирование объектов воздействия;
Возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, активных рабочих станций;
Возможность отображения сигнала тревоги на рабочей станции администратора безопасности, 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;
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;
Интеграция с локальным репутационным облаком, позволяющая приложению в режиме реального времени получать вердикт по запускаемой программе или файлу;
Централизованно управляться с помощью единой системы управления.

2.7. Программные средства антивирусной защиты и фильтрации спама для почтовых серверов.

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

Exim;
Zimbra;
Postfix;
Sendmail;
Microsoft Exchange и т.д.

2.7.2. Программные средства антивирусной защиты и фильтрации спама для почтовых серверов 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 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 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 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 внешней программой;
Возможность удаления (если удаление технически возможно) файлов, в которых обнаружены вредоносные составляющие, а также подозрительных файлов, перемещение и изолирование объектов воздействия;
Возможность блокирования доступа к зараженным файлам, в том числе полученным по каналам передачи данных, сервера, на котором обнаружены зараженные файлы;
Возможность оповещения администратора, в том числе до подтверждения его получения или до завершения сеанса;
Возможность восстановления функциональных свойств зараженных объектов.
Возможность получения и установки обновлений без применения средств автоматизации. В автоматизированном режиме с сетевого ресурса;
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 локальных 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;
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;
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 HTML, CSV, PDF;
Совместимость с DAG в Microsoft Exchange;
Поддержка ролей MS Exchange: Mailbox, Edge, Hub Transport, Client Access Server (CAS);
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;

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 локальных 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;
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;
Возможность фильтрации файлов Microsoft Office, содержащих макросы;
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;
Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
2.8. Требования к программным средствам централизованного управления, мониторинга и обновления.
2.8.1. Программные средства управления для всех средств защиты должны обеспечивать реализацию следующих функциональных возможностей:
Возможность отображения на рабочей станции администратора безопасности сигнала тревоги, идентифицирующего обнаруженные угрозы безопасности, рабочие станции и сервера, где они были обнаружены, и предпринятое антивирусным решением действие. Сигнал тревоги выдается при активном сеансе администратора безопасности до завершения сеанса;
Возможность получения и установки обновлений антивирусных баз в автоматизированном режиме с сетевого ресурса, автоматически через сетевые подключения;
Установка системы управления антивирусной защиты из единого дистрибутива;
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 работе антивирусной защиты;
Сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
Наличие различных методов установки антивирусных агентов: для удаленной установки – RPC, GPO;
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;
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;
Доступ к локальным репутационным облачным сервисам 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;
Поддержка функциональности управления шифрованием данных;
Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на

систему управления;
Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
Построение графических отчетов как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и т.д.;
Наличие преднастроенных стандартных отчетов о работе системы;
Экспорт отчетов в файлы форматов PDF, HTML, CSV и XML;
Возможность передачи событий из базы данных в IBM Qradar и HP Arcsight или по Syslog (RFC 5424);
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 Certificate Authority;
Наличие веб-консоли управления приложением;
Наличие системы контроля возникновения вирусных эпидемий.
2.9. Требования к программным средствам антивирусной защиты для виртуальных серверов.
2.9.1. Программные средства антивирусной защиты для виртуальных серверов должны функционировать на платформах виртуализации:
VMware NSX для vSphere 6.3, 6.2
VMware ESXi 6.0, 6.5, 6.7;
Windows Server 2012 R2 Hyper-V;
Windows Server 2016 Hyper-V;
Windows Server 2019 Hyper-V;
Citrix XenServer 7.1;
Платформа Proxmox VE: гипервизор Proxmox VE 5.4;
Huawei FusionSphere – FusionCompute CNA 6.3.1;
Скала-Р 7.0.6;
KVM на базе одной из следующих операционных систем:
Ubuntu Server 16.04, 18.04 LTS;
Red Hat Enterprise Linux Server 7,6;
CentOS 7.6;
2.9.2. Программные средства антивирусной защиты для виртуальных серверов должны функционировать на гостевых операционных системах:
Windows 10 Desktop Pro / Enterprise / LTSC / RS4 / RS5 / 19H1 (32 / 64-разрядная).
Windows 8.1 Update 1 Professional / Enterprise (32 / 64-разрядная).
Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-разрядная).
Windows Server 2019 Standard / Datacenter (в полном режиме) (64-разрядная).
Windows Server 2016 Standard / Datacenter (в полном режиме) (64-разрядная).
Windows Server 2012 R2 Standard / Datacenter / Essentials (в полном режиме) (64-разрядная).
Windows Server 2012 Standard / Datacenter / Essentials (в полном режиме) (64-разрядная).
Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (в полном режиме) (64-разрядная).
Debian GNU / Linux 9.8 (64-разрядная).
Debian GNU / Linux 8.11 (64-разрядная).
Debian GNU / Linux 8.11 i386 (32-разрядная).
Ubuntu Server 18.04 LTS (64-разрядная).
Ubuntu Server 16.04 LTS (64-разрядная).
CentOS 7.6 (64-разрядная).
CentOS 6.10 (64-разрядная).
Red Hat Enterprise Linux Server 8 (64-разрядная).
Red Hat Enterprise Linux Server 7.6 (64-разрядная).
Red Hat Enterprise Linux Server 6.10 (64-разрядная).
SUSE Linux Enterprise Server 15 (64-разрядная).
ALT Linux 8 (64-разрядная).
ALT Linux 7.0.6 (64-разрядная).
Oracle Linux 7.6 (64-разрядная).
Astra Linux SE 1.6 (без поддержки режимов Мандатного разграничения доступа и Замкнутой программной среды).
Astra Linux SE 1.5 (без поддержки режимов Мандатного разграничения доступа и Замкнутой программной среды).
2.9.3. Программные средства антивирусной защиты для виртуальных серверов должны обеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг;
Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
Наличие легких агентов для среды виртуализации для повышения производительности и уменьшения количества избыточных операций и данных.
Возможность многоуровневой постоянной защиты на базе машинного обучения.

Возможность регулировки использования веб-ресурсов виртуальными и удаленными рабочими станциями.
Возможность поддержки нескольких клиентов и контроль учетных записей на основе разрешений
Возможность присваивания запускаемым приложениям уровень доверия, для ограничения их доступа к критически важным ресурсам.
Возможность контроля целостности файлов для обеспечения неизменности критических системных компонентов и других важных файлов.
Возможность анализа поведения для отслеживания активности приложений и процессов.
Возможность обеспечения защиты от любых попыток шифрования критических данных, хранящихся в виртуальных средах.
Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
2.10. Требования к обновлению антивирусных баз.
2.10.1. Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:
Регламентное обновление антивирусных баз не реже 24 раз в течение календарного месяца;
Множественность путей обновления, в том числе – по каналам связи и на других носителях информации;
Проверку целостности и подлинности обновлений средствами электронной цифровой подписи.
3. Требования к оказанию услуг.
3.1. Общие требования:
Срок сервисной поддержки от производителя лицензионного программного обеспечения не менее 12 месяцев со дня надлежащей приемки Заказчиком Услуг;
Оценка ресурсов, необходимых для работы систем – предоставить план работ по внедрению, расчет времени, необходимого на внедрение и запуск в эксплуатацию систем;
Инсталляция компонентов контроля автоматизированных рабочих мест и серверов: установка серверной части программного обеспечения, контроль и проведение консультация по установке агентов на конечные устройства;
Поставщик должен предоставить Заказчику возможность контроля и надзора за ходом выполнения настроек;
Поставщик должен немедленно известить Заказчика и до получения от него указаний, приостановить настройки, при обнаружении:
- возможных неблагоприятных для Заказчика последствий выполнения его указаний о способе выполнения настроек;
- иных, не зависящих от Поставщика обстоятельств, угрожающих годности или качеству результатов внедрения Системы, либо создающих невозможность завершения их в срок.
Поставщик должен произвести консультацию по установке программного обеспечения серверной и клиентской части на территории заказчика, а также обеспечить сдачу системы под «ключ».
Потенциальный поставщик обязан предоставить лицензии согласно Приложению (Таблица 1).

4. Требования к поставщику:
Поставщик должен осуществить обучение трех сотрудников Заказчика по администрированию и настройки Программного обеспечения;
С целью исключения возможности поставки контрафактного программного обеспечения, Потенциальный поставщик должен предоставить в составе заявки авторизационное письмо от производителя поставляемого программного обеспечения (либо его уполномоченного территориального представителя) в адрес Заказчика, подтверждающее полномочность Потенциального поставщика производить работы по поставке, установке, настройке, доработке и предоставление гарантий на поставляемое программное обеспечение. Либо, Потенциальный поставщик должен иметь статус производителя, поставляемого программного обеспечения (в составе заявки необходимо представить соответствующие документы).

Приложение

Приложение к ТС.docx

Подписал	Саханов Булат Хасанович
Дата подписания	20.01.2021