Техническое задание

1. Продление неисключительных прав (продление лицензии) на использование программного обеспечения ESET NOD32 Business Edition renewal for 170 user

|  |  |  |
| --- | --- | --- |
| № п/п | Предмет контракта с указанием объема оказываемых услуг | Требования к качеству, техническим характеристикам услуг, требования к их безопасности и иные показатели, связанные с определением соответствия оказываемых услуг потребностям заказчика, максимальные и (или) минимальные значения показателей и показатели, предлагаемого к использованию при оказании услуг товара, значения которых не могут изменяться |
| 1 | Продление неисключительных прав (продление лицензии) на использование программного обеспечения защита почтового сервера NOD32-EMS-RN-1-250  | Антивирус и Антишпион Устранить все типы вредоносного программного обеспечения, в том числе вирусы, руткиты,черви и шпионские программы, а также проверяют репутацию приложений до запуска на базеоблачной технологии. Для более эффективного обнаружения вредоносных программ и быстрогосканирования облачные технологии Антиспам и Антифишинг Автоматически блокировать спам и фишинговые рассылки сразу после установкибез осуществления дополнительных настроек с высоким процентом определения.Локальный карантин Позволить системным администраторам просматривать подозрительные сообщения черезвеб-интерфейс и централизованно принимать меры. Системный администратор можетразрешить пользователю самому просматривать уведомления о помещении сообщенияв карантин и производить действия для одного сообщения или группы. Возможные действиязависят от причины, по которой сообщение было помещено в карантин.Сканирование базы данных по требованиюСнизить потребление ресурсов системы, выбирая для сканирования только нужныебазы данных или отдельные почтовые ящики.Правила для сообщений Расширенные настройки фильтрации почтовых сообщений позволяют определить действиядля каждого подозрительного сообщения. Параметры фильтрации включают стандартные поля(тема, отправитель, тело сообщения и заголовки). Поврежденные или защищенные паролемархивы и вложения проходят детальную проверку для определения реального типа файла,а не только расширения архива.Защита от эксплойтов Устранить вредоносное ПО, использующее уязвимости в самых распространенных программныхпродуктах, включая веб-браузеры, PDF-редакторы, почтовые клиенты, Microsoft Office и Java.Кроме того, блокировщик эксплойтов контролирует поведение процессов и выявляетподозрительную активность, которая является типичной для целевых атак и атак нулевого дня.Расширенноесканирование памятиТехнология позволяла обезвреживать зашифрованные вредоносные программы, которыеустанавливаются на компьютер скрыто от пользователя.HIPS Система предотвращения вторжений защищает от вредоносных программ и другойнежелательной активности, которая может негативно повлиять на безопасность компьютера.Расширенный анализ поведения в сочетании с возможностями сетевой фильтрациипо обнаружению позволяет отслеживать запущенные процессы, файлы и разделы реестра.Контроль устройств Автоматическое сканирование подключаемых внешних устройств и настройка правилработы со съемными носителями информации для каждого пользователя. Блокируетнесанкционированное подключение устройств к серверу. Позволяет создавать правила для групппользователей, соответствующие политикам безопасности компании. Тактично уведомляетпользователя о том, что подключенное устройство заблокировано, и дает дальнейшие инструкции.для Microsoft Exchange Server |
| 2 | Продление неисключительных прав (продление лицензии) на использование программного обеспеченияESET NOD32 Business Edition renewal for 170 user  | 1. Общие требования:

Предоставляемые неисключительные права (лицензии) на использование ПО включают в себя право на воспроизведение, ограниченное правом инсталляции, копирования и запуска, предоставляемое с единственной целью передачи этого права конечным пользователям.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: * лицензионный файл ключа;
* программные средства антивирусной защиты рабочих станций и серверов;
* программные средства централизованного управления, мониторинга и обновления на ОС Windоws, Linux/BSD/Solaris;
* обновляемые антивирусные базы данных;
* эксплуатационную документацию на русском языке.

Компоненты:- ESET Endpoint Antivirus,- ESET File Security для Microsoft Windows Server,- ESET File Security для Linux/BSD/Solaris,- ESET Mobile Security Business Edition, - ESET Remote Administrator1. Требования к программному обеспечению антивирусной защиты рабочих станций:

Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:• Microsoft Windows XP Professional;• Microsoft Windows Vista (32-bit и 64-bit),• Microsoft Windows 7 (32-bit и 64-bit),• Microsoft Windows 8 (64-bit)Программные средства антивирусной защиты рабочих станций под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:• резидентный антивирусный мониторинг;• антивирусное сканирование по команде пользователя или администратора;• защита от еще неизвестных вредоносных программ на основе эвристического анализа;• обнаружение руткитов (скрытых файлов/системных аномалий);• содержит Host Intrusion Prevention System (HIPS) для предотвращения попыток внешнего воздействия, а так же для мониторинга процессов, файлов и ключей реестра;• блокировка сменных носителей информации и устройств (USB); • интеграция с центром безопасности Windows;• самозащита антивирусных продуктов от вредоносных программ, злоумышленников или неквалифицированных пользователей;• проверка наличия актуальных обновлений системы;• системные требования к защите рабочих станций – 44 Мб RAM (на пиках нагрузок), HDD 40 Мб, 300 МГц Processor 32-bit (x86) и 64-bit (x64) Intel, AMD или 100% совместимые;1. Требования к программному обеспечению антивирусной защиты серверов:

Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:• Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003 все Service Packs, все текущие обновления;• Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition;• Microsoft Windows Server 2008, Standard, Microsoft Windows Server 2008 Datacenter, Microsoft Windows Server 2008 Enterprise, Microsoft Windows Server 2008 Standard, Microsoft Windows Server 2008.• Microsoft Windows Server 2008 R2 Standard Edition, Microsoft Windows Server 2008 R2 Enterprise Edition, Microsoft Windows Server 2008 R2 Datacenter Edition, Microsoft Windows Server 2008 R2 Foundation Edition.Программные средства антивирусной защиты файловых серверов под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:• резидентный антивирусный мониторинг;• антивирусное сканирование по команде пользователя или администратора;• защита от еще неизвестных вредоносных программ на основе эвристического анализа;• обнаружение руткитов (скрытых файлов/системных аномалий);• содержит Host Intrusion Prevention System (HIPS) для предотвращения попыток внешнего воздействия, а так же для мониторинга процессов, файлов и ключей реестра; • блокировка сменных носителей информации и устройств (USB); • интеграция с центром безопасности Windows;• самозащита антивирусных продуктов от вредоносных программ, злоумышленников или неквалифицированных пользователей;• проверка наличия актуальных обновлений системы;• проверка трафика по протоколам IMAP, POP3 независимо от используемого почтового клиента;• защита HTTP-трафика - проверка всех объектов, поступающих на компьютер пользователя по протоколу HTTP и FTP;• защита зашифрованного трафика – протоколы HTTPs, POP3s;• наличие системы централизованного сбора с клиентских рабочих мест потенциально опасных образцов вредоносного кода и возможность централизованно или вручную отправлять образцы вредоносного кода вирусным экспертам.1. Требования к системе управления антивирусной защитой:

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:• автоматизированное обновление программных средств антивирусной защиты и антивирусных баз;• доставка обновлений на рабочие места пользователей сразу после их получения;1. Требования к обновлению антивирусных баз:

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:• реализована возможность создания зеркала обновлений для экономии трафика;• зеркало обновлений можно создать на любом ПК сети;• типы обновлений: обновление БД сигнатур вирусов, программных компонентов, обновление ядра; • пакеты обновления зеркала можно загружать двумя способами: по протоколу HTTP (рекомендуется) и с помощью общего сетевого диска (SMB);• осуществляется проверка целостности и подлинности обновлений средствами электронной цифровой подписи. |