Приложение № 1 к Документации

УТВЕРЖДАЮ

Заместитель генерального директора
по организационным вопросам
АО «Институт «ЭНЕРГОСЕТЬПРОЕКТ»

(должность)

И.С. Золотарева

(подпись) *(ФИО)*

Техническое задание

Программное обеспечение должно быть лицензионным (Заказчику должно быть передано право на использование программного обеспечения на условиях простой (неисключительной) лицензии).

Программное обеспечение должно соответствовать всем действующим нормам (ГОСТам, ТУ и т. д.), а также иметь сертификаты соответствия (если данное программное обеспечение подлежит сертификации) и гарантии Лицензиата. Лицензиат должен иметь законные основания на предоставление прав на использование программного обеспечения Сублицензиату.

Программное обеспечение должно соответствовать нормам действующего законодательства РФ. Все программное обеспечение должно иметь официальный русифицированный интерфейс (быть русифицировано в соответствии со стандартами ISO). Все программное обеспечение должно поддерживать работу с кириллицей

№	Право-обладатель	Наименование программы для ЭВМ, право использования которой предоставляется Сублицензиату	Срок исполь-зования програм-мы для ЭВМ*	Кол-во ЭВМ, на которых возможно использова-ние программы*	Цена, руб.	Сумма, руб.
1.	Eset	Права на программу для ЭВМ ESET NOD32 Antivirus Business Edition renewal for 350 User	12 месяцев	350		
Итого общий размер лицензионного вознаграждения:						

* Если иное не установлено Типовым соглашением правообладателя с конечным пользователем и с учетом ограничений, установленных указанным соглашением, в соответствии с пунктами 2 и 3 статьи 1238 ГК РФ.

Антивирусные средства должны включать:

- Программные средства антивирусной защиты для рабочих станций Windows.
- Программные средства антивирусной защиты для файловых серверов Windows.
- Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows.
- Обновляемые базы данных сигнатур вредоносных программ и атак.
- Эксплуатационную документацию на русском языке.

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

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

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, 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. Автоматическое определение уровней ограничения на основании репутации программы.

• Наличие механизмов защиты от атак.

• 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.

• 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 обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

• Регламентное обновление антивирусных баз не реже 1 раза 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 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.

Начальник ОИТ С.В. Ванюшкин