«УТВЕРЖДАЮ»

Директор по безопасности –

начальник отдела безопасности

АО «НИИМЭ»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Довгань И.Д.

« » 2020 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

1. **Адрес поставки:** 124460, г. Москва, г. Зеленоград, ул. Академика Валиева, д. 6, стр.1
2. **Покупатель:** Акционерное общество «Научно-исследовательский институт молекулярной электроники» (АО «НИИМЭ»)

ИНН / КПП 7735579027 /773501001

ОГРН 1117746568829

1. **Предмет закупки и объем поставки.**

Поставка лицензионного программного обеспечения в следующем объеме:

|  |  |  |  |
| --- | --- | --- | --- |
| **№****пп** | **Наименование** | **Количество****почтовых ящиков** | **Срок лицензии** |
| 1 | Kaspersky Secure Mail Gateway | 700 | 1 год, начиная с 01.09.2020 г. |

**Поставка эквивалента не предусмотрена ввиду необходимости обеспечения взаимодействия антивирусного программного обеспечения Kaspersky Secure Mail Gateway c программным обеспечением, имеющимся у Заказчика.**

1. **Требования к системе антивирусной защиты почты** (далее - Система):

Система должна иметь возможность:

* функционировать в виде отдельного виртуального почтового шлюза;
* распространяться в виде шаблона виртуальных машин OVA
* интегрироваться в существующую почтовую инфраструктуру и анализировать сообщения электронной почты по протоколу SMTP.
* иметь плагин управления Системой совместимый с внедренным решением Kaspersky Security Center;
* иметь возможность проводить полную настройку функционирования системы через графический веб интерфейс;
* обнаруживать, блокировать и лечить зараженные сообщения электронной почты и зараженные вложения, удалять сообщения и вложения, помещать копии зараженных сообщений в хранилище;
* иметь возможность подключаться к инфраструктуре облачных служб производителя, предоставляющий доступ к базе вредоносной активности и репутаций файлов, интернет-ресурсов и программного обеспечения;
* обнаруживать и блокировать спам, предполагаемый спам, массовые рассылки (в том числе маркетинговые рассылки), удалять сообщения, помещать копии сообщений в хранилище;
* обнаруживать и блокировать сообщения, содержащие любые макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять сообщения или вложения, помещать копии сообщений в хранилище;
* обнаруживать и блокировать сообщения, содержащие зашифрованные объекты под паролем, удалять сообщения или вложения, помещать копии сообщений в хранилище;
* обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов (например, файлы формата ZIP, RAR, TGZ, 7z, QZIP), блокировать отдельные файлы внутри архивов;
* обнаруживать и блокировать фишинг или ссылки на вредоносные веб-сайты, удалять сообщения, помещать копии сообщений в хранилище;
* выполнять контентную фильтрацию сообщений по имени, размеру и типу вложений определять истинный формат и тип вложения, независимо от его расширения); удалять сообщения, содержащие вложения определенного формата или с определенным именем (в том числе внутри запакованных архивов), или сообщения, размер которых превышает допустимый, помещать копии сообщений в хранилище;
* выполнять настройку контентной фильтрацию сообщений по имени, размеру и типу вложений с помощью графического веб интерфейса.
* сохранять сообщения из хранилища в файл и пересылать сообщения получателям с помощью графических кнопок управления веб интерфейса;
* обрабатывать сообщения электронной почты согласно спискам правилам, заданным для групп отправителей и получателей;
* в правилах фильтрации сообщений электронной почты иметь возможность указывать пользователей и группы пользователей из Microsoft Active Directory® и generic LDAP для того, чтобы можно было осуществлять маршрутизацию сообщений для отдельных учетных записей и групп пользователей;
* уведомлять отправителя, получателей и администратора об обнаружении сообщений, содержащих зараженные, защищенные паролем и недоступные для проверки объекты;
* отправлять уведомления пользователям о результатах проверки их сообщений модулями программы;
* получать статистику работы программы по протоколу SNMP, включать и отключать отправку SNMP-ловушек;
* настраивать параметры и управлять работой программы через веб-интерфейс;
* отправлять и получать сообщения по защищенному каналу TLS/SSL;
* осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC;
* подписывать исходящие сообщения электронной почты с помощью технологии DKIM;
* добавлять примечания к исходящим и входящим сообщениям;
* добавлять предупреждения о небезопасном вложении к входящим сообщениям;
* осуществлять мониторинг состояния почтового трафика и использования ресурсов системы, просматривать списки последних обнаруженных угроз в веб-интерфейсе программы;
* иметь возможность просматривать журнал событий программы и загружать его на жесткий диск;
* иметь возможность обновляться через веб-интерфейс;
* иметь возможность просматривать через веб интерфейс программы хранилище зараженных писем, открывать в веб интерфейсе программы копии зараженных писем из хранилища;
* иметь возможность с помощью кнопок графического веб интерфейса задавать временные интервалы отображения списков зараженных писем, производить поиск по письмам;
* отправлять через веб интерфейс программы копии писем из хранилища почтовым получателям с помощью кнопок доставки графического веб интерфейса;
* сохранять копии зараженного письма из хранилища на локальный жесткий диск оператора антивирусного шлюза, с помощью кнопок сохранения графического веб интерфейса;
1. **Требования по комплектности Программного обеспечения:**
* необходимый набор серийных номеров либо ключевых файлов, лицензированных на 700 почтовых ящиков;
* дистрибутив Системы в формате шаблонов виртуальных машин OVA, либо ссылку на получение дистрибутива;
* файлы эксплуатационной документации.

СОГЛАСОВАНО:

Начальник ОИТ АО «НИИМЭ»

\_\_\_\_\_\_\_\_\_\_\_\_\_ Капичников Д.В.

Руководитель проектов по

информационной безопасности

АО «НИИМЭ»

\_\_\_\_\_\_\_\_\_\_\_\_\_ Григорьев Г.Н.