|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | № | **Требования к техническим характеристикам системы защиты электронных почтовых сообщений** | **Параметры предлагаемого оборудования** | **Соответствие / несоответствие требованиям** | **Для указания соответствия (необходимо указать точное расположение каталога/номер страницы вложенного файла для проверки соответствия)** |
| **Оборудование почтовой безопасности** | | | | | |
|  | | | Заполняется поставщиком | | |
| **Требования к техническим характеристикам и емкости** | 1 | Реализация в виде программно-аппаратного комплекса с поддержкой установки в стандартную телекоммуникационную стойку; | *Заполняется поставщиком* | *Заполняется поставщиком* | *Заполняется поставщиком* |
| 2 | Форм-фактор устройства: не более 1 RU; |  |  |  |
| 3 | Сетевые интерфейсы: не менее 4 портов 1Гбит/с разъем RJ-45; |  |  |  |
| 4 | Общий объем хранимой информации: не менее 2ТБ; |  |  |  |
| 5 | Блок питания: 100–240V AC, 60–50 Hz: не менее 2 шт. |  |  |  |
| **Функциональные требования** | 1 | Решение должно предоставлять собой шлюз безопасности электронной почты. |  |  |  |
| 2 | Решение должно поддерживать работу в режимах: |  |  |  |
| 3 | -Почтовый сервер; |  |  |  |
| 3.1. | -Шлюз (агент MTA); |  |  |  |
| 3.2. | -Прозрачный шлюз (желательно); |  |  |  |
| 3.3. | Решение должно обеспечивать Анти-спам фильтрацию электронной почты; |  |  |  |
| 4 | Решение должно обеспечивать Анти-фишинг фильтрации электронной почты; |  |  |  |
| 5 | Решение должно обеспечивать Антивирусная фильтрации электронной почты; |  |  |  |
| 6 | Решение должно обеспечивать фильтрацию URL в теле электронных писем; |  |  |  |
| 7 | Решение должно обеспечивать Предотвращение утечек конфиденциальных данных; |  |  |  |
| 8 | Решение должно обеспечивать Карантин для электронной почты; |  |  |  |
| 9 | Решение должно обеспечивать фильтрацию входящей и исходящей электронной почты; |  |  |  |
| 10 | Решение должно поддерживать до 100 почтовых доменов; |  |  |  |
| 11 | Решение должно поддерживать политики защиты и маршрутизация почты на основе атрибутов LDAP (домена); |  |  |  |
| 12 | Решение должно поддерживать SMTP-аутентификацию посредством LDAP, RADIUS, POP3 или IMAP; |  |  |  |
| 13 | Решение должно поддерживать очередь сообщений для ошибочных, поврежденных, задержанных и недоставленных сообщений; |  |  |  |
| 14 | Решение должно обеспечивать возможность интеграции с внешними RBL (Realtime Blackhole List) сервисами; |  |  |  |
| 15 | Решение должно поддерживать технологии Email аутентификации: Domain Key Identified Management (DKIM), Sender Policy Framework (SPF); |  |  |  |
| 16 | Решение должно обеспечивать поддержку «черных» и «белых» списков отправителей (email адрес\email домен\IP адрес); |  |  |  |
| 17 | Решение должно обеспечивать поддержку технологии Greylisting («серые списки»); |  |  |  |
| 18 | Решение должно обеспечивать защиту от DDoS атак на почтовую инфраструктуру; |  |  |  |
| 19 | Решение должно обеспечивать контроль URL в теле письма; |  |  |  |
| 20 | Решение должно поддерживать интеграцию с внешними аппаратными или облачными решениями класса Sandbox (песочница), для осуществления эффективной защиты от угроз класса “0-day”. Письмо, содержащее подозрительные вложение не должны перенаправляться на принимающий почтовый сервер до окончания инспекции (с положительным заключением) на решении класса Sandbox; |  |  |  |
| 21 | Предотвращение утечек конфиденциальных данных. Идентификация и блокировка контента должна быть возможна, как минимум, по ключевым словам, словарям, регулярным выражениям, хэшу файла; |  |  |  |
| 22 | Контроль содержимого электронных писем (по типу, числу, размеру вложений); |  |  |  |
| 23 | Наличие на устройстве защищенного веб-портала, позволяющего осуществлять переписку без прямой отправки защищаемого контента получателю; |  |  |  |
| 24 | Решение должно поддерживать экспорт журналов событий; |  |  |  |
| 25 | Решение должно поддерживать мониторинг по протоколу SNMP; |  |  |  |
| 26 | Решение должно обеспечивать возможность архивирования входящих и исходящих сообщений на основе политик с поддержкой резервных копий на отчуждаемых носителях; |  |  |  |
| 27 | Решение должно обеспечивать поддержку отказоустойчивых кластеров в режимах Active-Active, Active-Passive; |  |  |  |
| 28 | Решение должно обеспечивать встроенную, основанную на политиках, маршрутизацию почты и управление очередями; |  |  |  |
| 29 | Решение должно поддерживать карантин сообщений электронной почты; |  |  |  |
| 30 | Решение должно поддерживать архивирование входящих и исходящих сообщений; |  |  |  |
| 31 | Наличие защищенной операционной системы; |  |  |  |
| 32 | Администрирование решения должно выполняться через графический веб-интерфейс управления или интерфейс командной строки (CLI); |  |  |  |
| 33 | Количество защищаемых почтовых ящиков или пользователей не должно быть ограничено лицензией (желательно); |  |  |  |
| 34 | Решение должно обеспечивать эвристические методы фильтрации; |  |  |  |
| 35 | Решение должно обеспечивать фильтрацию вложений/содержимого; |  |  |  |
| 36 | Решение должно обеспечивать усиленную проверка заголовков сообщения; |  |  |  |
| 37 | Решение должно обеспечивать проверку в реальном времени на спам с помощью «черных» списков URL (SURBL); |  |  |  |
| 38 | Решение должно обеспечивать проверку в реальном с использованием Байесовского статистического фильтра (желательно); |  |  |  |
| 39 | Решение должно обеспечивать фильтрацию, по запрещенным словам; |  |  |  |
| 40 | Решение должно обеспечивать управление спамом (принять, передать, отклонить или отвергнуть), основанное на блоклисте проверок контрольных сумм спама SHFSH; |  |  |  |
| 41 | Решение должно обеспечивать сканирование и анализ графических изображений; |  |  |  |
| 42 | Решение должно обеспечивать поддержку общих и пользовательских настраиваемые «черные»/«белые» списки; |  |  |  |
| 43 | Решение должно обеспечивать поддержка «черных» списков, формируемых в реальном времени (RBL), третьих фирм (желательно); |  |  |  |
| 44 | Решение должно обеспечивать проверку на ложность IP-адреса; |  |  |  |
| 45 | Решение должно обеспечивать проверку с использованием грейлистинга; |  |  |  |
| 46 | Решение должно обеспечивать различные действия при выявлении спама, включая маркировку писем; |  |  |  |
| 47 | Решение должно обеспечивать проверку на вирусы SMTP-сообщений; |  |  |  |
| 48 | Решение должно обеспечивать поддержку сжатых присоединенных файлов и вложенных архивов; |  |  |  |
| 49 | Решение должно обеспечивать помещение зараженных файлов на карантин; |  |  |  |
| 50 | Решение должно обеспечивать поддержку уведомлений при замене сообщений; |  |  |  |
| 51 | Решение должно обеспечивать фильтрацию вложений; |  |  |  |
| 52 | Решение должно обеспечивать проверку и блокирование по типам файлов; |  |  |  |
| 53 | Решение должно поддерживать антивирусный движок и сигнатуры для него собственной разработки (от производителя); |  |  |  |
| **Требования к протоколированию, уведомлению и отчетности** | 1 | Решение должно обеспечивать протоколирование изменения конфигураций и событий управления; |  |  |  |
| 2 | Решение должно обеспечивать протоколирования вирусных инцидентов; |  |  |  |
| 3 | Решение должно обеспечивать протоколирование активности модуля противодействия спаму; |  |  |  |
| 4 | Решение должно обеспечивать поддержку внешнего Syslog-сервера; |  |  |  |
| 5 | Решение должно обеспечивать расширенную систему отчетности с поддержкой устройств; |  |  |  |
| 6 | Решение должно обеспечивать уведомление о критических событиях и вирусных инцидентах; |  |  |  |
| 7 | Решение должно позволять изменять содержимое уведомлений о событиях и инцидентах; |  |  |  |
| 8 | Решение должно поддерживать полноценную систему отчетности, включающая генерацию отчетов по категориям; |  |  |  |
| 9 | Решение должно поддерживать предустановленные шаблоны отчетов; |  |  |  |
| 10 | Решение должно обеспечивать формирование отчетов по расписанию; |  |  |  |
| 11 | Решение должно обеспечивать формирование и отправку отчетов в PDF-формате; |  |  |  |
| **Требования к производительности** | 1 | Производительность маршрутизации электронной почты на типовых сообщениях размером 100Кб: не менее 90000 писем в час; |  |  |  |
| 2 | Производительность маршрутизации электронной почты с антивирусной и антиспам проверкой на типовых сообщениях размером 100Кб: не менее 90000 писем в час; |  |  |  |
|  | 3 | Требования к подпискам и технической поддержке: |  |  |  |
|  | 4 | Срок поддержки оборудования производителем в режиме 24х7: не менее 3 лет. |  |  |  |
|  | 5 | Срок действия подписок на обновления антивируса, антиспама, сервиса кибер­аналитики, облачной песочницы, защиты кликов URL, обнаружение подложного отправителя: не менее 3 лет. |  |  |  |
| **Комплектация** | 1 | заводское крепление для монтажа в серверный шкаф типа RACK 19-дюймов. Power cord cable c13-c14 - 2 шт |  |  |  |
| **Ед. изм.** | **комплект** | | | | |
| **Количество** | **2** | | | | |