e-mail: info@uzairways.com
tel: +998 (78) 140-46-23
fax: +998 (71) 236-75-00

www.uzairways.com

UZBEKISTAN airways

Aksiyadorlik jamiyati | Joint-Stock Company

УТВЕРЖДАЮ:
Вр.и.о. Первого заместителя
Председателя Правления
АО «UZBEKISTAN AIRWAYS»

_____ **Xusanov U.A.**
«20» 12 2021 г.

Техническое задание на приобретения оборудования по обеспечению защиты электронных почтовых сообщений

O'zbekiston, Toshkent,
Amir Temur shohko'chasi, 41
GSP-100060

Uzbekistan, Tashkent,
41, Amir Temur avenue
GSP-100060

Аннотация

Данное Техническое задание определяет общие требования к техническому решению, составу и техническим характеристикам оборудования, необходимое для приобретения решения по защите электронных сообщений.

Цель технического задания

Основной целью технического задания является формирование законченного предложения, созданного на основе технических и иных требований, представленных далее по тексту документа.

Предпосылки к внедрению современных средств защиты электронной почты

Основные предпосылки к внедрению средств защиты электронной почты:

1. Отсутствие современных средств и инструментов защиты электронных почтовых сообщений;
2. Текущая информационная инфраструктура не предусматривает надлежащий контроль за передачей электронной почты, включая инспекцию, контентную фильтрацию и блокировку нежелательных почтовых сообщений.

Задачи технического задания

Задачами настоящего технического задания, являются описание основных и дополнительных требований по следующим компонентам:

1. Утверждение функциональных требований к системе защиты электронных сообщений;
2. Утверждение требований к протоколированию, уведомлению и отчетности системы защиты электронных сообщений;
3. Утверждение требований к техническим характеристикам решения;
4. Утверждение требований к производительности решения;
5. Утверждение требований к сервисным подпискам и поддержке.

Источники финансирования

Собственные средства АО «Uzbekistan Airways»

Минимальные требования к поставляемым компонентам

Перечень и количество закупаемого оборудования и сопутствующего программного обеспечения

Наименование	**Количество**
Система защиты электронных сообщений	2 комплекта

Требования к техническим характеристикам системы защиты электронных почтовых сообщений

Минимальные функциональные требования:

1. Решение должно предоставлять собой шлюз безопасности электронной почты.
2. Решение должно поддерживать работу в режимах:
   -Почтовый сервер;
   -Шлюз (агент MTA);
   -Прозрачный шлюз (желательно);
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);

Минимальные 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;

Минимальные требования к техническим характеристикам и емкости:

1. Реализация в виде программно-аппаратного комплекса с поддержкой установки в стандартную телекоммуникационную стойку;
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.

Минимальные 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 24x7: не менее 3 лет.
5. Срок действия подписок на обновления антивируса, антиспама, сервиса кибер-аналитики, облачной песочницы, защиты кликов URL, обнаружение подложного отправителя: не менее 3 лет.

Дополнительные требования

Всё поставляемое оборудование должно покрываться гарантией от производителя, позволяющей получать обновления программного обеспечения поставляемых компонентов, и производить замену вышедшего из строя оборудования, в течении трех лет со дня поставки оборудования.

ТРЕБОВАНИЯ К ПОСТАВКЕ

Место поставки	Склад Департамента закупок АО «UZBEKISTAN AIRWAYS», 100167, г.Ташкент, Международный аэропорт Ташкент им.И.Каримова, тел +/998 71/ 255-05-51, 255-68-37, факс + /998 71/ 255-35-24, e-mail: procurement@uzairways.com)
Требования к новизне	Закупаемое оборудование и лицензии должно быть новым, ранее не использованным, не эксплуатируемым, не восстановленным, не являться выставочным образцом, произведенным не ранее 2021 года, не снятым с производства, не иметь дефектов.
Требования к сроку поставки	Максимальный срок поставки товара – 60 банковских дней с момента заключения договора.
Условия оплаты	15% после подписания договора в течении 10 календарных дней, 85% по факту поставки товара в течение 10 календарных дней
Сервисный центр	Наличие сервисного центра, выполняющего гарантийное обслуживание товара (требуется официальное письмо компании-производителя с указанием авторизованного сервисного центра) о готовности выполнять гарантийное обслуживание товара не менее 36 (тридцати шести). Либо аналогичные способы сервисной поддержки.
Авторизация производителя	Наличие у поставщика письменного разрешения на продажу товара на территории Республики Узбекистан (требуется официальное письмо компании-производителя об авторизации поставщика)
Сертификат соответствия	Поставляемый товар должен иметь сертификат соответствия, выданный уполномоченным органом Республики Узбекистан.

РАЗРАБОТАНО:
Начальник Управления
информационной безопасности **Kirillov A.A.**

С О Г Л А С О В А Н О:

Директор по цифровизации **Xodjiyev Sh.G.**

и.о. Директор Департамента закупок **Sidikov A.Z.**

Директор Департамента по поддержки и развитию IT инфраструктуры **Fazilov X.N.**