«УТВЕРЖДАЮ»

Председатель правления

АКБ «Банк Развития Бизнеса»

\_\_\_\_\_\_\_\_\_\_\_\_ С.С. Аннакличев

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

на модернизацию сервисов корпоративной электронной почты АКБ «Банк Развития Бизнеса»

СОГЛАСОВАНО

Руководитель

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность, наименование предприятия)

\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Подпись ФИО

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.

г. Ташкент, Узбекистан, 2025

1. **Наименование проекта**

Модернизация сервисов корпоративной электронной почты в АКБ «Банк Развития Бизнеса».

1. **Информация об участниках проекта**

**Заказчик:** АКБ «Банк развития Бизнеса»

**Исполнитель: -** будет определен по результатам тендера

1. **Назначение и цель проекта**

Проект направлен на модернизацию сервисов корпоративной электронной почты для повышения уровня кибербезопасности и защиты от современных угроз. Основные задачи включают интеграцию решений для защиты электронной почты и анализа угроз с существующей почтовой инфраструктурой на базе **Zimbra Mail Server**.

**В рамках модернизации планируется:**

* **Усиление защиты от спама и фишинговых атак** путем фильтрации нежелательных сообщений, аутентификации отправителей при помощи механизмов SPF, DKIM и DMARC), а также проверки ссылок в письмах.
* **Блокировка вредоносных вложений** с использованием антивирусных механизмов и детального анализа файлов в изолированной среде (песочнице).
* **Настройка маршрутизации почтового трафика** через систему защиты электронной почты с учетом политики безопасности компании и обеспечения совместимости с **Zimbra Mail Server**.
* **Внедрение механизмов предотвращения утечек данных** для защиты конфиденциальной информации при отправке электронной почты.
* **Фильтрация и анализ почтового трафика на уровне “песочницы”**, включая контроль аномальной активности и выявление потенциальных угроз.
* **Продление и увеличение количества подписок на Zimbra Mail Server** для обеспечения стабильной работы почтовой инфраструктуры с учетом роста нагрузки и количества пользователей.



1. **Техническая часть отбора наилучшего предложения**

Качество поставляемой продукции должно соответствовать требованиям, указанным в техническом задании (далее ТЗ).

Количество и объем предоставляемого товара и объем оказываемой услуги согласно ТЗ.

* 1. **Плановые сроки поставки товаров и проведения интеграционных работ**

Срок поставки товаров: не позднее 105 календарных дней с момента подписания договора.

Сроки проведения интеграционных работ: не более 14 рабочих дней

* 1. **Место поставки и проведения работ**

Местом поставки и проведения работ является офис Заказчика, расположенный по адресу: г. Ташкент, улица Навои 18А.

* 1. **Технические требования к поставляемой продукции**

|  |  |  |
| --- | --- | --- |
| **Система защиты электронной почты** | **Архитектура и форм-фактор:*** Виртуальная машина, развернутая на серверах Банка;
* Возможность развертывания любого количества виртуальных устройств без необходимости дополнительного лицензирования виртуальных машин. Таким образом должна присутствовать возможность развертывания любого количества виртуальных машин без потери производительности;

**Основные функциональные требования:*** Решение защиты электронной почты должно лицензироваться в соответствии с количеством пользователей, которые используют фильтр антиспам, антивирус, защита от 0-day атак.
* Решение защиты электронной почты должно иметь функционал антиспам, антивирус, защита от атак 0-day, защита от фишинга, защита от spoofing, предотвращение утечки информации (DLP), фильтрацию отправителей на основе репутации домена, IP-адреса.

**Производительность:*** Решение защиты электронной почты должно быть лицензировано на 2800 пользователей.

**Требования к OC и архитектуре:*** Решение защиты электронной почты должно представлять собой виртуальную машину, которая построена на защищенной и специализированной операционной системе.
* Шлюз не должен использовать open source MTA (или любой переработанный open source MTA, как send mail, qmail или postfix) для минимизации влияния возможности эксплуатации известных уязвимостей распространенных open-source продуктов.
* Решение должно поддерживать технологию виртуальных шлюзов, когда на одном устройстве можно настроить виртуальные адреса, и использовать эти адреса в качестве исходящие IP для отправки сообщений (примечание: технологии виртуализации не рассматриваются как технологии виртуальных шлюзов в этом контексте).
* Технология виртуальных шлюзов должна давать возможность разделять почтовый шлюз на несколько виртуальных адресов шлюзов, из которых нужно отправлять или получать почту. Каждый виртуальный шлюз должен подлежать настройке IP-адреса, имени хоста, домена и почтовой очереди.
* Технология виртуальных шлюзов должна давать возможность администратору определить listener, который привязан к виртуальному шлюзу с настройкой индивидуальных контрольных установок для каждого шлюза.

**Требования к безопасности:*** Решение должно иметь возможность проверять на предмет спуфинга доменов. Если отправитель попытается подделать домен, сообщение должно быть удалено или отправлено в карантин. Шлюз должен поддерживать верификацию SPF, DKIM и DMARC.
* Решение должно иметь механизмы защиты от подделки имен в поле "From:" e -mail, учитывая возможные вариации имен.
* Решение должно иметь встроенные механизмы для защиты от атак Denial of Service с помощью различных методов, включая (но не ограничиваясь) следующими:
* Осуществление контроля SMTP сессии и ограничения трафика в соответствии с IP адресом отправителя, доменов, репутацией и адресом отправителя конверта;
* Назначение максимального количества SMTP сессий на IP адрес отправителя;
* Назначение максимального количества сообщений на соединение, максимального количество получателей в час, максимального количества неправильных получателей в час.
* Шлюз должен иметь возможность защиты от атак класса исследования каталога с помощью различных методов, включая, но не ограничивая следующее:
* Интеграция с AD или LDAP каталогами для идентификации неправильных получателей. Должны поддерживаться запросы в реальном времени и не использоваться синхронизация записей, чтобы не сталкиваться с проблемой рассинхронизации.
* Управление максимальным количеством Bounce сообщений в час в соответствии с IP адресом отправителя, доменом или репутацией.
* Решение должно поддерживать LDAP запросы включая, но не ограничивая следующее:
* Осуществление LDAP доменных запросов, при которых шлюз может использовать различные LDAP сервера, ассоциированные с различными доменами, для запуска LDAP запросов, которые назначены на один и тот же listener (домен A будет осуществлять LDAP запросы на LDAP сервер А, а домен Б будет осуществлять запросы на LDAP сервер Б)
* Осуществление LDAP запросов по цепочке, когда шлюз должен запускать серию из LDAP запросов (LDAP1 затем LDAP2 и т.д.), пока результат не будет положительным или последний запрос не покажет отрицательный результат)
* Возможность обойти запросы LDAP Accept для определенных получателей, если для них невозможно запустить LDAP.
* Решение должно поддерживать маршрутизацию LDAP, маскирования (email NAT) LDAP.
* Решение должно поддерживать т. н. "Проверка рикошетов" ("Bounce Verification), при которой все исходящие сообщения помечаются с помощью цифровой метки для того, чтобы обеспечить фильтрацию bounce атак на шлюзе.
* Решение должно включать защиту от cross-site request forgeries (CSRF), XSS и других атак на web интерфейс.
* Система должна иметь возможность нативно интегрироваться с “Песочницей” без использования REST API.
* В систему должен быть интегрирован модуль предотвращения утечек информации (DLP).
* Модуль DLP должен классифицировать информацию на основе:
* Слов или фраз
* Регулярных выражений
* Словарей
* Предопределенного шаблона, определяющий общие типы конфиденциальных данных
* Политики DLP должны позволять Администратору настроить главное и второстепенное действие в случае нарушение политики.
* Главное действие должно включать:
* Доставка письма получателю
* Отправка в карантин
* Блокировка письма

Второстепенное действие должно включать: * Отправка копии письма в любой пользовательский карантин или карантин "Политика".
* Изменение заголовка темы.
* Добавление в сообщение текста
* Отправка сообщения на альтернативный почтовый хост.
* Отправка скрытой копии сообщения.
* Отправка уведомления о нарушении DLP отправителю или другим контактам.

**Требования к управлению почтового трафика:*** Решение должно поддерживать контроль как входящего, так и исходящего трафика на одном устройстве, используя подключение одним или несколькими интерфейсами.
* Решение должно позволять настройки политик email для входящих и исходящих писем и настраивать системы антиспам, антивирус, фильтры контента, фильтра 0-day.
* Решение должно позволять создание различных политик на основе различных комбинаций отправителей, получателей, LDAP групп отправителей, LDAP групп получателей.
* Шлюз должен обеспечивать единый графический интерфейс управления с возможностью просмотра всех политик для простого управления.
* Решение должно иметь возможность применять политики на основе различных групп отправителей, включая, но не ограничивая следующее:
* Черные списки по IP, домена или репутации.
* Белые списки по IP, домена или репутации.
* Посторонние Realtime Blackhole list (RBLs).
* Посторонние Open Relay Blacklist (ORBLs).
* Белые и черные списки отправителей и получателей.
* Шлюз должен иметь возможность заблокировать или ограничить "плохих" отправителей и определить индивидуальные политики для отправителей (как внутренних, так и внешних) с помощью различных методов, включая, но не ограничивая следующее:
* IP отправителя, диапазон IP;
* домен;
* репутация;
* DNS список.
* Шлюз должен иметь возможность ограничивать email трафик по IP адресу, домена, репутации, адрес отправителя конверта с помощью различных методов. Включая, но не ограничивая следующее:
* Максимальное количество получателей в час.
* Максимальное количество получателей в единицу времени (на основе адреса отправителя конверта).
* Решение должно использовать настройки детальных политик email включая, но не ограничивая следующее:
* Просмотр обратного DNS домена и назначения политик.
* Максимальные настройки политик отправителей.
* Максимальное количество сообщений на соединение;
* Максимальное количество получателей на соединение;
* Максимальный размер сообщения;
* Максимальное количество одновременных сессий на IP адрес;
* Включение TLS и опции включения;
* SMTP аутентификация и опции включения.
* Шлюз должен иметь возможность осуществлять фильтрацию вложений с помощью различных методов, включая, но не ограничивая следующее:
* Файл. Сообщение содержит файл, имя которого совпадает с регулярным выражением;
* Расширение файла. Сообщение содержит файл с определенным расширением.
* MIME тип - сообщение содержит файл определенного MIME типа.
* Шлюз должен предлагать возможность отправлять сообщения в карантин, отправлять дубликат в карантин, вырезать вложенные файлы, отправить скрытую копию или перенаправить почту на другой хост или другому получателю, заменить целое сообщение или только присоединенный файл с определенным шаблоном сообщения.
* Политики обработки email в предложенном шлюзе должны иметь возможность проверять отправителя для IP адреса, DNS PTR и адреса отправителя конверта, а также иметь таблицы исключений.
* Решение должно позволять индивидуальный доступ к различным карантинам для различных пользователей, включая доступ к Policy / Virus карантин.
* Решение должно иметь возможность настройки фильтров контента как с GUI, так и с CLI.
* Фильтры CLI должны включать скриптовый язык, что позволяет администраторам строить сложные структуры if-then-else с целью экономии вычислительных ресурсов решения защиты электронной почты, фильтруя письма до задействования основных сканирующих механизмов, таких как антиспам, антивирус и т.д. Для достижения максимальной гибкости фильтры должны быть применимы как входящему, так и исходящему трафику почты.
* Шлюз должен поддерживать словари с весовыми коэффициентами. Для каждого объекта в словаре клиент может определить термин "вес", и определить предельное значение срабатывания исходя из суммы весовых коэффициентов.
* Решение должно поддерживать выявления email атак в определенный период времени с определенным количеством сообщений:
* С одной и той же темой за последний час;
* С одним и тем же отправителем конверта за последний час.
* Решение должно поддерживать выявления Graymail и помещать в карантин подобные письма

**Требования к системе защиты от спама:*** Решение должно фильтровать спам с помощью набора различных методов, включая, но не ограничивая следующее:
* Интегрированный антиспам фильтр в устройство.
* Двухуровневый подход к фильтрации спама с репутационным фильтром в качестве первого уровня и контентным антиспам фильтром в качестве второго уровня.
* Поддержка более чем одного антиспам фильтра.
* Настройка различных политик защиты от спама для различных пользователей
* Технология репутационной фильтрации (Sender IP / domain) на одном устройстве.
* Технология обнаружения спам контента на основе контента.
* Технология адаптивного обучения для эффективной защиты от snow shoe спама.
* Технология глобальной репутационной фильтрации должна иметь возможность блокировать отправителя на этапе подключения без загрузки и анализа полного листа перед определением репутации отправителя.
* Репутация отправителя должна кэшироваться определенное время.
* Шлюз должен как минимум 1 раз в 5 мин обновлять правила антиспам.
* Шлюз должен иметь возможность изменения политик в реальном времени на основе домена, IP адреса и обновлять политики в реальном времени для блокировки / ограничение плохих отправителей.
* Решение должно администрироваться с минимальными усилиями без постоянной "подстройка" и "подгонки правил", создание антиспам правил вручную.
* Решение должно иметь специализированный карантин для спама и обеспечивать индивидуальный контроль доступа пользователей к этому карантина.
* Решение должно обеспечивать списки, настраиваемые пользователем (Safelist/ Blocklist). Каждый пользователь индивидуально управляет своим списком.
* Решение должен консолидировать в карантине спам-письма для пользователей, имеющих несколько email адресов.
* Решение должно поддерживать как локальные (на отдельных устройствах), так и глобальный (для нескольких устройств) анти-спам карантин.
* Решение должно регулярно отправлять оповещение пользователям при попадании писем в спам-карантин.
* Содержание оповещения должно настраиваться.
* В оповещении должна содержаться ссылка на письма в карантине.
* В предлагаемом решении должны быть плагины для популярных groupware решений (Outlook, Notes и пр.). Эти плагины должны поддерживать предоставление отчетов о пропущенном спам, ложные срабатывания, фишинг и вирусы.
* Решение должно поддерживать дополнительные языки для карантина спама для конечных пользователей. В частности, должна присутствовать обязательно поддержка русского языка.

**Требования к антивирусу (anti-malware):*** Решение должно иметь функционал сканирования на вирусы, интегрированный в устройство.
* Решение должно поддерживать более одного антивирусного механизма и каждое сообщение должно сканироваться несколькими механизмами.
* Шлюз должен обеспечивать защиту от атак 0-day для того, чтобы блокировать целевые email атаки в дополнение к 0-day вирусным атакам.
* Решение должно обеспечивать динамичный карантин, куда отправляются подозрительные на вирус сообщение до тех пор, пока не появится вирусная сигнатура или пока не закончится максимальное время хранения сообщений.
* Решение должно иметь возможность загружать сигнатуры автоматически по расписанию.
* Решение должно сканировать сжатые и архивные файлы.
* Решение должно обеспечивать защиту от распространяющегося спама, фишинга, атак 0-day и предотвращать пользователей от загрузки malware или распространение важной информации.
* Фильтр защиты от атак 0-day должен перезаписывать URL в сообщениях для того, чтобы защитить клиентов от посещения вредоносных веб-узлов и добавления сообщений о вреде ссылки.
* Решение должно идентифицировать файловые угрозы во входящих сообщениях на основе репутации файла, анализа файла в песочнице или изменения вердикта.
* Решение должно поддерживать определения репутации URL в письмах и категории URL в письмах.
* Решение должно иметь возможность выявления офисных документов популярных форматов (ms office, OLE и XML) c макросами и определения для них отдельных правил обработки.
* Система должна иметь возможность интеграции с Endpoint Security решением этого же производителя. В рамках интеграции система защиты корпоративной почты должна получать список разрешенных/запрещенных файлов от Endpoint Security и иметь возможность ретроспективного анализа.

**Требования к администрированию:*** Шлюз должен иметь возможность предоставления набора отчетов и журналов, включая, но не ограничивая следующее:
* Графический монитор входящей и исходящей почты за последний час, день, неделю, месяц.
* Список обработки email.
* Отчеты потоков email (список всех сообщений на конкретного получателя за определенный период времени с деталями, как принималось и обрабатывалось сообщения).
* Статистика email и пропускная способность.
* График пропускной способности системы для среднего и максимального количества сообщений в очереди, общее количество входящих соединений и сообщений, среднее количество сообщений, средний размер сообщений и общий размер сообщений, загрузка системы в целом и по процессам, и возможность иерархического просмотра всех вышеперечисленных отчетов.
* Шлюз должен поддерживать несколько DNS серверов с различными методами, включая, но не ограничивая следующее:
* Поддержка как Internet Root DNS, так и локальных DNS серверов.
* Поддержка нескольких DNS серверов в соответствии с доменами назначения
* Решение должно обеспечивать возможность централизованного отслеживания сообщений для двух или более устройств с использованием различных критериев поиска (отправитель, получатель, время, репутация, результаты работы фильтров и т.д.).
* Решение должно иметь возможность построение централизованных отчетов, включая, но не ограничивая следующее:
* Централизованные отчеты для нескольких устройств
* Отчет для всех сообщений или для группы доменов
* Отчет по объему почты для пользователей (top n получателей для спама, вирусов, общего количества почты, размером сообщений)
* Отчет об объеме почты для домена (top входящей и исходящей почты для домена, спама и вирусов)
* Отчет о нарушении политик или контентному фильтра.
* Отчет об эффективности Outbreak
* Отчет о входящих и исходящих вирусах
* Решение должно обеспечивать полные исторические детали о сообщении в поиске. Должна предъявляться полная информация о сообщении, включая IP адрес, репутацию отправляющей системы, результаты сканирования на спам, вирусы и.т.д.
* Решение должно обеспечивать отчеты, доступные в PDF и CSV форматах.
* Решение должно обеспечивать мониторинг системы с помощью следующих протоколов:
* SNMP v2 / v3
* MIB-II
* XML
* Syslog
* Решение должно отправлять предупреждения в виде SNMP и email предупреждений.
* Решение должно иметь интерфейсы HTTPS, SSH.
* Решение должно иметь функционал централизованного управления встроенного в консоль с возможностью управления несколькими устройствами в режиме peer2peer и синхронизацией конфигурации по всей системе.
* Решение должно иметь различные методы обновлений, включая, но не ограничивая следующее:
* Системные обновления. с возможностью восстановления почтовых сервисов в течение 5 минут.
* Обновления антиспам механизма
* Обновления антивируса
* Автоматические обновления Outbreak (0-day вирусов)
* Решение должно иметь встроенный функционал поддержки через GUI с возможностью отправки детальной информации в службу техподдержки.
* Решение должно включать возможность возвращения базовой ОС на предыдущую версию в случае неудачного обновления.
* Решение должно иметь функционал делегированного администрирования с гибким контролем пользователей и пользовательских ролей.
* Решение должно обязательно поддерживать графический интерфейс на русском языке.

**Гарантия и сервисная поддержка:*** В поставку должно быть включены все необходимые для работы системы лицензии
* В поставку должна быть включена техническая поддержка производителя уровня Basic сроком на 36 месяцев;
* Условия сервисной поддержки должны включать в себя возможность регистрации сервисных случаев в режиме 24х7х365
* В поставку должна быть включена техническая поддержка L1 от поставщика сроком на 12 месяцев.
* Лицензии для Anti-Spam, DLP, Outbreak Protection, Anti-Virus, Anti-Malware сроком на 36 месяцев в количестве 2800 штук.
* Наличие официального сервисного центра производителя на территории Республики Узбекистан.

**Прочее:*** Производитель решения по защите электронной почты не должен входить в международные санкционные списки, признанные международными санкционными органами, а также национальные санкционные списки страны Заказчика.
 | **2 шт.** |
| **Песочница** | **Архитектура и форм-фактор:*** Физический сервер для установки в стандартный монтажный шкаф 19 ", высота 1U

**Сетевые интерфейсы:*** Не менее 3 x 1 GbE, RJ45.
* Не менее 4 x 10 GbE, SFP +.
* В комплект поставки должен был включен SFP трансивер стандарта RJ-45.

**Производительность:*** Процессор Intel Xeon(R) Gold 6330N CPU @ 2.20GHz (2шт) или его аналог
* Оперативная память не менее 512 GB DDR4-3200-MHz
* Решение должно использовать специализированный гипервизор, на котором работает защищенная виртуальная среда с защитой от обнаружения среды виртуализации.
* Количество сканируемых файлов в день: не менее 600.

**Методы получения файлов:*** Интеграция с межсетевым экраном с функциями защиты от современных сетевых угроз (Next Generation Firewall, NGFW)
* Интеграция с системой безопасности Web-трафика;
* Песочница должна поддерживать нативную интеграцию с системой защиты электронной почты
* Возможность ручной загрузки файлов;
* С помощью встроенного API.

**Администрирование:*** Поддержка WebUI и CLI
* Создание нескольких учетных записей администратора
* Конфигурация резервного копирования и восстановления файлов
* E-mail оповещение при обнаружении вредоносного файла

**Сетевые возможности / Развертывание*** Возможность развертывания в режиме без подключения к Интернет (AirGap)
* В песочнице должен быть отдельно выделенный “чистый” интерфейс для интеграции с системой защиты корпоративной почты.
* В песочнице должен быть отдельно выделенный “грязный” интерфейс для исходящих соединений, в том числе для соединений, которые инициируются со стороны вредоносного ПО.

**Функциональные возможности*** Песочница должна выполнять статический, динамический, криминалистический и расширенный поведенческий анализ.
* Песочница должна детектировать и проводить анализ файлов с отложенным исполнением.
* В процессе анализа вредоносных программ песочница должна фиксировать индикаторы CnC соединения.
* В процессе анализа песочница должна фиксировать все DNS запросы, все HTTP соединения и другие сетевые потоки. Должна быть доступна вся история сетевых соединений в формате PCAP.
* Результаты анализа должны быть доступны в форматах JSON, STIX, CSV и в виде правил Snort.
* У пользователя должна быть возможность напрямую взаимодействовать с анализируемыми файлами в безопасной виртуальной среде через специальный интерфейс.
* Решение должно выдавать результаты анализа в форме графической панели или отчета, показывает детали поведения угрозы и должно как минимум включать:
* Операции ОС системного уровня
* API вызовы
* Работы процессов / потоков
* криптографические операции
* Возможности по защите от debuggers
* Возможности противодействия "засыпанию" malware или задержке времени
* Модификации файловой системы
* Модификации реестра
* Сетевые порты и протоколы
* характеристики протоколов
* Экспорт в PDF
* В отчете должна содержаться видеозапись анализа файла. У пользователя должна быть возможность воспроизвести видеозапись в платформе или же скачать ее.
* В песочнице должны быть методы защиты обхода песочниц со стороны вредоносного ПО.

**Поддержка типов файлов для анализа*** PE32: .EXE, .DLL
* PE32 +: .EXE, .DLL
* Java Archives (.JAR)
* JavaScript (.JS)
* Portable Document Format (.PDF)
* Office Documents (.DOC, .DOCX, .RTF, .XLS, .XLSX, .PPT, .PPTX)
* XML Based Office Document Types (.DOCX, .XLSX, .PPTX)
* XML - Extensible Markup Language (.XML)
* Архивы и карантины:
* ZIP (.ZIP)
* Quarantine (.VBN, .SEP)
* xz (.xz), gzip (.gz), bzip2 (.bz2), tar (.tar)
* Mime HTML Files (.MHTML)
* Flash Files (.SWF)
* URLs
* MSI - Microsoft Installer files (.MSI)
* LNK - Windows shortcut files (.LNK)
* Batch (.BAT)
* HTML Application (.HTA)
* Powershell (.PS1)
* Visual Basic Script (.VBS)
* Windows Script File (.WSF)
* Encoded JavaScript (.JSE)
* Encoded Visual Basic (.VBE)
* Compiled HTML Help (.CHM)

**Гарантия и сервисная поддержка*** Оборудование должно обеспечиваться гарантией от производителя и сервисной поддержкой сроком не менее 36 месяцев.
* Условия сервисной поддержки должны включать в себя возможность регистрации сервисных случаев в режиме 24х7х365, обновление микрокода системы и версий установленного программного обеспечения.
* Наличие официального сервисного центра производителя на территории Республики Узбекистан.

**Прочее:*** Производитель решения не должен входить в международные санкционные списки, признанные международными санкционными органами, а также национальные санкционные списки страны Заказчика.
 | **1 шт.** |
| **Лицензии Zimbra Professional**  | В комплект поставки должны быть включены бессрочные лицензии Zimbra Network – Professional Edition и техническая поддержка уровня Стандарт со сроком на 36 месяцев.  | **1800 шт** |
| **Продление технической поддержки Zimbra** | В комплект поставки должна быть включена техническая поддержка на имеющиеся лицензии Zimbra Network – Professional Edition сроком на 36 месяцев.  | **1000 шт** |

1. **Гарантия и сервисная поддержка оборудования**

Оборудование должно обеспечиваться гарантией от производителя и сервисной поддержкой сроком не менее 36 месяцев.

Условия сервисной поддержки должны включать в себя возможность регистрации сервисных случаев в режиме 24х7х365, обновление микрокода системы и версий установленного программного обеспечения.

Наличие официального сервисного центра производителя на территории Республики Узбекистан.

1. **Требования к уровню технической поддержки со стороны Исполнителя**

В поставку должна быть включена техническая поддержка L1 на систему защиты электронной почты и песочницу от поставщика сроком на 12 месяцев.

Формат предоставления технической поддержки L1

**Удалённая техническая поддержка**, включая:

* Прием, регистрацию и первичную обработку инцидентов.
* Оценку критичности инцидента и эскалацию при необходимости.
* Диагностику и предоставление рекомендаций по устранению неисправностей.
* Контроль выполнения работ, информирование Заказчика о статусе запроса.
* Контроль процесса устранения инцидента, эскалация на L2/L3 при необходимости.
* Поддержку в установке обновлений и патчей.
* Организацию онлайн-консультаций с инженерами при необходимости.

**Классификация инцидентов и время реакции:**

* + - **P1 (Критический)** – Недоступность сервиса, угроза безопасности. Время реакции: **до 4 часов**.
		- **P2 (Средний)** – Проблемы отдельных пользователей, вопросы конфигурации. Время реакции: **до 8 часов**.
		- **P3 (Низкий)** – Консультации, запросы на изменение конфигурации. Время реакции: **до 24 часов**.

**Дополнительные требования:**

* Наличие инженера со знанием **узбекского и английского языков** для взаимодействия с пользователями и ведения коммуникации по техническим вопросам.

##  **Требования к Исполнителю**

##  **Квалификационные требования**

## Подтвердить участие в проекте со стороны Поставщика не менее 1 (одного) сертифицированного инженера уровня Эксперт и не менее 1 (одного) инженера уровня Профессионал по сертификации от производителя предлагаемого оборудования, предоставив действующие сертификаты.

##  **Прочие требования к Исполнителю**

В рамках выделенного бюджета Исполнитель должен выполнить следующие требования:

* Предоставить полностью укомплектованное и работоспособное оборудование, необходимое для обеспечения полноты использования запрашиваемой конфигурации;
* Исполнитель должен поставить новое (не бывшее в употребление), не восстановленное (refurbished), работоспособное оборудование, произведенное не раньше 2025 года и не снятое с производства на данный период;
* Поставка выполняется в полном объеме в адрес Заказчика (Представителя заказчика);
* Продукция должна соответствовать всем техническим требованиям и параметрам, указанным в пункте технического задания 4.3 «Технические требования к поставляемой продукции».
* Исполнитель должен предоставить авторотационное письмо (Manufacturer Authorization Form, МАФ) от уполномоченного представителя производителя, подтверждающее право поставлять товар на территории Республики Узбекистан;

## **Требования к интеграционным работам и обучению**

В состав поставки должны быть включены услуги по обучению 3-х инженеров Заказчика по администрированию Системы защиты электронной почты и песочницы.

В состав поставки должны быть включены услуги по внедрению решения Системы защиты электронной почты и песочницы инженерами Поставщика.

## **Требования к документации проекта**

В рамках выполнения работ Заказчику должны быть предоставлены Исполнителем нижеперечисленные документы:

* Техническая документация от производителя оборудования;
* Исполнительная документация проекта со включением отчета по тестированию
* Акт приемки в промышленную эксплуатацию.