SERVIKO LIMITED / Для размещения в Astana Hub

Техническое задание

Централизация управления корпоративной почтой и защита данных

Обновлённая редакция от 3 ноября 2026 года

1. Цель и исходная проблема

Создать управляемую корпоративную почтовую среду SERVIKO LIMITED для около 15 почтовых ящиков с едиными правилами доступа, защиты, резервного копирования и сохранения деловой переписки.

Исходные сервисы: Gmail, Mail.ru и почтовые сервисы хостинг-провайдеров. Размещение почты на разных платформах затрудняет централизованное администрирование, контроль прав и восстановление данных. Фактические настройки, принадлежность учётных записей и риски необходимо подтвердить аудитом.

Ожидаемый результат

Почтовые ящики включены в согласованный контур управления; уполномоченные администраторы управляют пользователями и доступом; переписка перенесена и проверена; резервное восстановление и отключение сотрудника подтверждены испытаниями.

Границы и условия

Точное число ящиков, домены, объёмы, состав данных и целевая платформа уточняются после аудита. Возможные варианты архитектуры: Google Workspace, Microsoft 365, Zoho Mail либо иное обоснованное решение. Ни одна платформа или интеграция не считается заранее выбранной.

Стоимость, лицензии, сроки и наличие доступов в настоящем ТЗ не утверждаются. Они определяются отдельно по результатам аудита и согласования объёма работ. Документ описывает планируемые требования, а не выполненное внедрение.

2. Требования к решению

Управление и работа с почтой

• Единый административный контур для согласованного перечня корпоративных ящиков; реестр пользователей, адресов, алиасов и ответственных лиц.

• Приём и отправка писем из согласованных клиентов и веб-интерфейса; поддержка необходимых общих адресов и делегированного доступа без совместного использования паролей.

• Сохранение писем, вложений, дат и доступных метаданных. Папки и метки сопоставляются по согласованным правилам; дубликаты и исключения отражаются в отчёте.

• Контакты, календари, фильтры и подписи включаются в перенос только после инвентаризации и согласования: их переносимость не предполагается автоматически.

Безопасность и права

• MFA для администраторов и сотрудников; порядок подключения, восстановления и замены факторов. Исключения оформляются и компенсируются согласованными мерами.

• Роли: владелец системы со стороны компании, администратор, сотрудник и, при необходимости, аудитор с доступом только к журналам. Принцип минимальных прав; административная учётная запись отделена от повседневной.

• Шифрование каналов связи; защита резервных копий; журналирование входов, изменений прав, административных действий и операций восстановления в пределах возможностей выбранного решения.

• Отзыв устаревших сессий, токенов, паролей приложений и лишних делегирований. Настройка антиспама, защиты от фишинга и правил внешней пересылки по согласованной политике.

Резервное копирование и восстановление

Предусмотреть резервное копирование почты с контролем успешности, уведомлениями об ошибках и защитой от несанкционированного удаления. Синхронизация и корзина не заменяют резервную копию. По результатам аудита согласовать периодичность, сроки хранения, место хранения, допустимую потерю данных (RPO) и время восстановления (RTO). Проверить восстановление отдельного письма с вложением и согласованного набора данных ящика.

Увольнение или смена роли сотрудника

По заявке уполномоченного лица заблокировать вход, отозвать активные сессии и токены, убрать делегирования и факторы доступа. Сохранить корпоративную переписку по принятой политике; передать доступ назначенному ответственному. Пересылку и автоответ включать только по согласованию. Удаление ящика допускается после проверки сохранности данных и разрешения владельца системы.

3. Источники данных и интеграции

Источники обследуются только в отношении корпоративных данных, разрешённых компанией к обработке. Пароли, токены, закрытые ключи и коды восстановления не включаются в ТЗ или общедоступные отчёты.

Данные для аудита и переноса

• Gmail, Mail.ru и почта хостинг-провайдеров: письма, вложения, папки/метки, доступные заголовки и настройки; контакты и календари - при включении в объём.

• Панели почтовых сервисов: учётные записи, алиасы, группы, делегирования, пересылки, квоты, методы аутентификации и доступные журналы.

• DNS-зоны корпоративных доменов: действующие MX, SPF, DKIM и DMARC; сведения о регистраторах и администраторах доменов.

• Согласованный список сотрудников и ответственных, сведения о клиентах почты, устройствах, резервных копиях и системах, отправляющих письма от имени компании.

Потенциальные способы подключения

• **IMAP/SMTP:** IMAP рассматривается для чтения и переноса писем; SMTP - для отправки и проверки почтового потока. Условия подключения, шифрование, аутентификация и ограничения подтверждаются для каждого сервиса.

• **Gmail API:** возможная работа с данными Gmail при подтверждённой доступности и предоставленных разрешениях. Объём OAuth-доступа и способ авторизации выбираются по результатам аудита.

• **Microsoft Graph:** возможная интеграция с почтой и учётными записями Microsoft 365, если эта платформа выбрана и необходимые функции доступны.

• **Zoho Mail API:** возможная интеграция с Zoho Mail при выборе платформы и подтверждении доступных функций, тарифных условий и разрешений.

• **DNS MX/SPF/DKIM/DMARC:** маршрутизация почты и аутентификация отправителей. Изменения выполняются по утверждённому плану с проверкой всех легитимных отправителей; политика DMARC вводится поэтапно после анализа результатов.

Перечисленные API и протоколы являются вариантами, а не обязательным одновременным набором. Исполнитель после аудита документирует выбранные интеграции, ограничения, квоты, требуемые права и резервный способ переноса. Наличие API, административных прав и доступа к DNS заранее не предполагается.

4. Этапы выполнения и результаты

Этап 1. Аудит

Инвентаризировать около 15 ящиков, домены, владельцев, объёмы и зависимости. Проверить доступные методы подключения, MFA, резервные копии и настройки DNS. Выявить личные учётные записи, ограничения и данные вне согласованного объёма. Результат: реестр, карта текущей инфраструктуры, перечень рисков и необходимых разрешений.

Этап 2. Проектирование

Сравнить применимые решения и согласовать целевую архитектуру, роли, политики безопасности, резервного копирования и хранения. Подготовить план миграции, сопоставление папок и адресов, окно переключения, порядок отката, критерии проверки и перечень интеграций. Согласовать сроки, бюджет и лицензирование отдельно до закупок и внедрения.

Этап 3. Пилот на 2–3 ящиках

Выбрать согласованные ящики, по возможности представляющие разные исходные сервисы. Настроить управление, MFA и права; перенести данные; проверить отправку, приём, резервное копирование, восстановление и отключение пользователя. Зафиксировать ошибки и ограничения. Результат: протокол пилота и решение о переходе к миграции. При нерешённых критических ошибках масштабирование не выполняется.

Этап 4. Миграция

Создать исходную резервную копию или подтверждённый экспорт, выполнить начальный перенос и сверку. Переключать ящики по согласованным группам, при необходимости менять DNS. Выполнить завершающую синхронизацию, проверить входящую и исходящую почту и отслеживать ошибки. Сохранять исходную среду до подтверждения полноты переноса и окончания согласованного периода отката.

Этап 5. Тестирование

Провести проверки по критериям приёмки, включая внешние адреса, вложения, права, MFA, восстановление и увольнение сотрудника. Сопоставить результаты с исходным реестром и нормативами RPO/RTO. Устранить дефекты и повторить затронутые проверки. Результат: итоговый протокол испытаний и реестр согласованных исключений.

Этап 6. Передача и завершение

Передать компании управление, документацию и инструкции; обучить ответственных лиц. Секреты передать по защищённому согласованному каналу. Отозвать временные доступы исполнителя; удалить рабочие выгрузки в согласованном порядке после подтверждения сохранности данных. Результат: комплект документации и акт приёмки.

5. Критерии приёмки

Проверки выполняются по утверждённому перечню ящиков. Результаты, дата, ответственный и доказательства фиксируются в протоколе. Согласованные исключения должны быть явно перечислены.

• **Полнота охвата:** все ящики из утверждённого реестра включены в целевую систему; адреса, алиасы и ответственные соответствуют согласованной схеме.

• **Полнота переноса:** выполнена сверка количества писем по папкам/меткам и доступных объёмов с учётом преобразований. Проверены выборочные письма разных периодов, вложения и поиск. Нет необъяснённых потерь; расхождения и дубликаты документированы и согласованы.

• **Почтовый обмен:** для каждого ящика успешны отправка и получение внутри компании и с внешним адресом; проверены ответы и вложения. Настройки маршрутизации и результаты SPF/DKIM/DMARC подтверждены тестовыми письмами для согласованных потоков.

• **Доступ:** MFA включена для согласованных пользователей и администраторов; положительные и отрицательные тесты ролей подтверждают отсутствие лишних прав. Порядок восстановления доступа проверен.

• **Резервирование:** копирование выполняется по согласованному расписанию, ошибки обнаруживаются; восстановлены тестовое письмо с вложением и согласованный набор данных. Измеренные показатели соответствуют утверждённым RPO/RTO и срокам хранения.

• **Увольнение:** тестовый пользователь теряет возможность входа и использования проверяемых сессий/токенов; переписка сохранена и доступна назначенному ответственному в рамках его прав.

• **Передача:** компания получила инструкции, административное управление и результаты испытаний; временные доступы исполнителя отозваны. Открытых критических дефектов нет; прочие замечания имеют согласованный порядок устранения.

6. Комплект передаваемых материалов

Реестр ящиков и доменов; схема целевой архитектуры; перечень выбранных интеграций и прав; план и отчёт миграции; протоколы пилота и испытаний; настройки DNS без закрытых ключей; инструкции по пользователям, MFA, увольнению, резервированию и восстановлению; реестр исключений и акт приёмки.

7. Порядок согласования

Компания назначает владельца системы и подтверждает права на домены и корпоративные данные. Исполнитель готовит технические решения и результаты проверок. Доступы предоставляются уполномоченными лицами в минимально необходимом объёме. Изменения состава работ, платных услуг, сроков и критериев приёмки согласуются до выполнения соответствующих действий.