Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Корпоративная почта юрлица: свой сервер или облако в 2026

Наша методология: mailcow (Postfix + Dovecot + Rspamd) на VPS против облака — выбор и внедрение

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Почта юрлица ломается двумя способами: письма с домена падают в спам у Mail.ru и Gmail (теряются счета и заказы), либо компания сидит на бесплатных ящиках и теряет переписку вместе с уволенным сотрудником. Мы разбираем, когда офису до 50 PM достаточно облака, а когда нужен свой сервер, и как мы разворачиваем mailcow с полным DNS-контуром доставляемости.

Почему это важно бизнесу

- Письмо со счётом в спаме = потерянная сделка; о недоставке узнают через дни, когда клиент уже ушёл
- Переписка — актив компании: без своего домена и контроля ящиков её уносит любой уволенный менеджер
- Отказ сервера без внешнего бэкапа = безвозвратная потеря всей корпоративной истории писем
- Свой сервер без сопровождения дороже облака: простой 4–24 часа при сбое ложится на бизнес
- Тайна переписки (юристы, бухгалтерия) в чужом облаке — риск, который надо принимать осознанно

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

3.10

ветка Postfix в актуальном стеке mailcow; smtpd_relay_restrictions закрыт от open relay из кор...

mailcow-dockerized 2026-07

2048 бит

длина RSA-ключа DKIM; запись v=DKIM1 с селектором публикуем в DNS до первого отправленного пис...

генерация в UI mailcow, подпись — Rspamd dkim_signing

p=reject

целевая политика DMARC; включаем поэтапно none → quarantine → reject за 3–4 недели по rua-отчё...

наш стандарт (RFC 7489)

10/10

порог приёмки доставляемости на mail-tester перед сдачей сервера клиенту в эксплуатацию

наш стандарт приёмки

20 писем

порог алерта по deferred-очереди Postfix: выше — Telegram-алерт дежурному инженеру

наш стандарт мониторинга

1.2+

минимум TLS на SMTP/IMAP: smtpd_tls_mandatory_protocols = >=TLSv1.2, сертификат — автопродление

по докам Postfix 3.10

РЕАЛИЗАЦИЯ 1 ИЗ 3

Развёртывание mailcow: от чистого VPS до боевого сервера

Что настраиваем

VPS 4 vCPU / 8 ГБ / 100 ГБ SSD у российского хостера, Debian 12, до 50 ящиков на домене клиента

Как мы это делаем

1. До оплаты VPS выясняем у хостера два пункта: открыт ли исходящий порт 25 и ставят ли PTR-запись на mail.domain.ru — без них сервер бесполезен
2. Ставим Docker и mailcow-dockerized: generate_config.sh, MAILCOW_HOSTNAME=mail.domain.ru, docker compose up -d — стек Postfix 3.10 / Dovecot 2.3 / Rspamd / SOGo
3. TLS автоматом: контейнер acme-mailcow получает Let's Encrypt на mail.*, autodiscover.*, autoconfig.*; проверяем SAN в выданном сертификате
4. DNS-контур: MX, SPF «v=spf1 mx -all», DKIM 2048 бит из UI mailcow, DMARC p=none с rua на служебный ящик; TTL 300 на время отладки
5. Приёмка: 10/10 на mail-tester, тестовые письма в Gmail/Mail.ru/Яндекс, в заголовке Authentication-Results — pass по SPF, DKIM и DMARC

РЕЗУЛЬТАТ

Сервер уходит в эксплуатацию за 4–5 рабочих дней предсказуемо: весь стек — один compose-проект, обновляется штатным update.sh, конфигурация лежит в mailcow.conf и UI, а не размазана по системе. Новый инженер принимает площадку за час.

КЛЮЧЕВОЙ НЮАНС

PTR и порт 25 проверяем до покупки VPS: часть провайдеров режет 25-й порт навсегда или не делегирует обратную зону — тогда никакая настройка Postfix доставляемость не спасёт.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Доставляемость: DNS-контур, прогрев IP и постмастеры

Что настраиваем

Домен клиента + внешний IP сервера; охватываем SPF/DKIM/DMARC, репутацию IP и обратную связь Mail.ru/Gmail

Как мы это делаем

1. Проверяем историю IP до запуска по DNSBL (Spamhaus, Barracuda): «грязный» IP меняем у хостера сразу, а не отмываем неделями
2. SPF строго: v=spf1 mx ip4:x.x.x.x -all и не больше 10 DNS-lookup; все легальные отправители (сайт, CRM, 1С) инвентаризуем и заносим в запись
3. DMARC поэтапно: p=none на 2 недели, разбор rua-отчётов (кто реально шлёт от имени домена), затем quarantine, затем reject
4. Регистрируем домен в Постмастере Mail.ru и Google Postmaster Tools — репутацию и жалобы видим там раньше, чем их заметят клиенты
5. Прогрев нового IP: первые 2 недели ограничиваем исходящий поток, массовые рассылки на корпоративный сервер не пускаем вовсе

РЕЗУЛЬТАТ

Письма стабильно доходят в inbox у всех трёх больших приёмников РФ; подделку домена режут сами получатели по DMARC, а деградацию репутации мы видим по rua-отчётам и постмастерам за дни до первых жалоб пользователей.

КЛЮЧЕВОЙ НЮАНС

Маркетинговые рассылки никогда не гоняем через корпоративный сервер: одна кампания портит репутацию IP на недели и валит обычную переписку. Под рассылки — отдельный IP или сервис.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Эксплуатация: бэкап, мониторинг очереди, антиспам

Что настраиваем

Боевой mailcow до 50 ящиков; резервный контур на втором хосте + Zabbix и Telegram-алертинг

Как мы это делаем

1. Бэкап штатным helper-scripts/backup_and_restore.sh (vmail, mysql, redis, crypt) по cron в 03:00, копия — на второй хост через borg, retention 14 дней
2. Zabbix: триггер на deferred-очередь Postfix (>20 писем — алерт в Telegram) и ежесуточная проверка IP по DNSBL
3. Rspamd: greylisting для незнакомых отправителей, обучение bayes переносом писем в Junk (sieve), пороги add_header/reject не трогаем без статистики
4. Защита доступа: netfilter-контейнер mailcow банит перебор паролей SMTP/IMAP; клиентам — app-пароли и TLS-only, порт 25 только для MTA-трафика
5. Раз в квартал восстанавливаем один ящик из бэкапа на стенде: бэкап без теста восстановления считаем несуществующим

РЕЗУЛЬТАТ

RPO по переписке — 24 часа; о застрявшей очереди узнаём за минуты из Telegram, а не через три дня от клиентов. При отказе VPS поднимаем сервер из бэкапа на новом хосте за 3–4 часа с тем же IP-контуром DNS.

КЛЮЧЕВОЙ НЮАНС

Мониторим не «сервер жив», а deferred-очередь и репутацию: SMTP может отвечать 250 OK, пока вся исходящая почта тихо копится в deferred из-за блокировки на стороне получателя.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Порт 25 закрыт хостером**
  Многие VPS-провайдеры блокируют исходящий 25-й порт по умолчанию; проверяем до покупки и открываем тикетом заранее, иначе сервер не отправит ни письм…

- ✕ **Нет PTR-записи на IP**
  Mail.ru отвергает почту с IP без обратной зоны; PTR ставит только хостер — запрашиваем mail.domain.ru до первого отправленного письма.

- ✕ **SPF с ~all и лишними include**
  softfail пропускает подделки, а >10 DNS-lookup даёт permerror; держим v=spf1 mx ip4:… -all и пересчитываем lookup после каждого include.

- ✕ **DMARC p=reject с первого дня**
  Мгновенный reject режет легальные потоки (сайт, 1С, CRM), о которых забыли; сначала p=none и две недели разбора rua-отчётов.

- ✕ **Бэкап на том же диске**
  Отказ VPS уносит и ящики, и «бэкап» разом; выгрузку backup_and_restore.sh обязательно уводим на второй хост через borg или rsync.

- ✕ **Рассылки с корпоративного IP**
  Одна маркетинговая кампания загоняет IP в DNSBL и валит обычную переписку; рассылки — только с отдельного IP или через внешний сервис.

- ✕ **Миграция без imapsync**
  Ручной перенос через почтовый клиент теряет папки, флаги и часть писем; imapsync переносит инкрементально, сотрудники работают без простоя.

- ✕ **Забытые «прочие» отправители**
  Формы сайта и 1С шлют мимо SPF/DKIM и падают в спам; инвентаризуем все источники и заводим их в SPF либо через авторизованный relay сервера.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Домен компании вместо бесплатных @mail.ru; все ящики — под контролем организации
- SPF -all, DKIM 2048 бит, DMARC p=none с rua — обязательны даже в облачном варианте
- Облако (Яндекс 360) при 5–15 PM без особых требований к тайне переписки
- Регулярный экспорт критичной переписки imapsync в архив — хотя бы раз в месяц

НОРМАЛЬНО

- mailcow на VPS РФ-хостера: PTR, открытый порт 25, TLS через acme-контейнер
- Ежесуточный backup_and_restore.sh с копией на второй хост, retention 14 дней
- DMARC доведён до quarantine; домен заведён в постмастеры Mail.ru и Google
- Мониторинг deferred-очереди и DNSBL с алертами в Telegram

ХОРОШО

- DMARC p=reject с регулярным разбором rua; MTA-STS и TLS-RPT на домене
- Резервный MX на втором сервере — приём почты при отказе основного
- Квартальный тест восстановления ящика из бэкапа на стенде
- Отдельный IP/сервис под рассылки; корпоративный сервер — только переписка

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] SPF на домене заканчивается на -all и включает все легальные источники (сайт, CRM, 1С)?
- [ ] DKIM-подпись 2048 бит стоит и даёт pass в заголовке Authentication-Results?
- [ ] DMARC доведён хотя бы до quarantine, и rua-отчёты кто-то реально читает?
- [ ] У IP сервера есть PTR-запись, совпадающая с hostname в HELO Postfix?
- [ ] Бэкап ящиков хранится вне сервера, и восстановление проверялось за последний квартал?
- [ ] Есть алерт на рост deferred-очереди Postfix, или о проблеме узнаете от клиентов?
- [ ] IP сервера проверяется по DNSBL автоматически, а не после жалоб на недоставку?
- [ ] При увольнении сотрудника ящик блокируется, а переписка остаётся у компании?
- [ ] TLS на SMTP/IMAP не ниже 1.2, и сертификат продлевается автоматически?
- [ ] Массовые рассылки отделены от корпоративного потока по IP и домену отправки?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Разворачиваем mailcow под ключ за 4–5 дней: VPS, DNS-контур, TLS, приёмка 10/10 на mail-tester
- Мигрируем ящики с Яндекс 360 / Exchange / хостинга через imapsync без простоя сотрудников
- Настраиваем SPF/DKIM/DMARC и выводим домен из спама у Mail.ru и Gmail
- Берём сервер на сопровождение: бэкапы, мониторинг очереди и репутации IP, алерты в Telegram
- Считаем TCO облака и своего сервера на 3 года под ваш профиль и честно советуем вариант

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Postfix Configuration Parameters (postconf 5) (postfix.org — 3.10)

02 Dovecot Core — настройки IMAP/аутентификации (doc.dovecot.org — 2.3)

03 Rspamd — модуль dkim_signing (rspamd.com — 4.x)

04 mailcow: dockerized — Backup & Restore, Update (docs.mailcow.email — 2026)

05 RFC 7489 — DMARC (datatracker.ietf.org — 2015)

06 Постмастер Mail.ru — справка отправителя (postmaster.mail.ru — 2026)

07 Шаблон деплоя почтового сервера ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.