Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Корпоративная почта на Postfix: SPF, DKIM, DMARC

Разворачиваем Postfix 3.11 + Rspamd 4.1: аутентификация домена, антиспам и измеримая доставляемость

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Письма компании молча падают в спам или режутся reject'ом у Gmail и Mail.ru: счета не доходят до контрагентов, КП — до клиентов, а отправитель узнаёт об этом последним. Мы разворачиваем связку Postfix + Rspamd с полной аутентификацией домена (SPF, DKIM, DMARC, PTR) и контуром мониторинга репутации — так, чтобы доставляемость была измеримой величиной, а не лотереей.

Почему это важно бизнесу

- Потерянный счёт или КП — это прямые деньги: сорванные оплаты и сделки, о которых компания даже не узнаёт
- Домен без DMARC p=reject открыт для фишинга «от директора»: поддельное письмо главбуху проходит фильтры
- Gmail с 2024 года требует SPF+DKIM+DMARC от массовых отправителей — без записей рассылки режутся на входе
- Попадание IP в Spamhaus останавливает переписку со всеми контрагентами разом; делистинг — от часов до нескольких дней и только после устранения причины
- Репутация домена копится месяцами, а теряется за день — восстановление дороже правильной настройки

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

3.11.5

актуальная стабильная ветка Postfix — на неё ведём новые внедрения, legacy-ветки получают только патчи

postfix.org, июль 2026

<0.3 %

жёсткий потолок spam rate по требованиям Google; наш рабочий ориентир в Postmaster Tools — ниже 0.1 %

Google Sender Guidelines

2048 бит

RSA-ключ DKIM (rspamadm dkim_keygen -b 2048): дефолтные 1024 бита уже не считаются надёжными

RFC 8301, доки Rspamd

10

лимит DNS-механизмов в SPF: одиннадцатый include даёт permerror и провал всей проверки

RFC 7208 §4.6.4

300 с

задержка greylisting в Rspamd (timeout=5min по умолчанию): ботнет не повторяет отправку через 5 минут, легитимный MTA — повторяет

доки Rspamd, greylisting

4/6/15

пороги действий Rspamd (greylist/add_header/reject) — наша стартовая калибровка actions.conf

Rspamd actions.conf

РЕАЛИЗАЦИЯ 1 ИЗ 3

Аутентификация домена: SPF → DKIM → DMARC

Что настраиваем

DNS-зона домена + Rspamd на MX; охватываем все источники отправки: MX, CRM, 1С, сайт

Как мы это делаем

1. SPF: v=spf1 ip4:<IP MX> + include для облачных сервисов, старт с ~all; считаем DNS-механизмы — не больше 10 (RFC 7208)
2. DKIM: rspamadm dkim_keygen -s 2026 -d domain -b 2048 -k /var/lib/rspamd/dkim/…; права 0600, владелец _rspamd
3. dkim_signing.conf: path="$domain.$selector.key", use_domain="header", allow_hdrfrom_mismatch=false
4. Интеграция milter: smtpd_milters=inet:127.0.0.1:11332, milter_protocol=6, milter_default_action=accept
5. DMARC поэтапно: p=none + rua-отчёты 2 недели → p=quarantine на месяц → p=reject; adkim/aspf оставляем relaxed

РЕЗУЛЬТАТ

Подделка From-домена перестаёт доходить до сотрудников, а Gmail, Mail.ru и Outlook видят полностью аутентифицированный поток: pass rate по SPF/DKIM держится выше 99 %

КЛЮЧЕВОЙ НЮАНС

Переход на p=reject делаем только после разбора rua-отчётов: в них всплывают забытые легитимные источники — CRM, 1С, сканеры — которые иначе молча отвалятся

РЕАЛИЗАЦИЯ 2 ИЗ 3

Периметр MX: postscreen, greylisting, TLS

Что настраиваем

Postfix 3.11 + Rspamd 4.1 + Redis на входящем MX; фильтрация до очереди и в milter

Как мы это делаем

1. postscreen: postscreen_dnsbl_threshold=2, postscreen_dnsbl_sites=zen.spamhaus.org*3 b.barracudacentral.org*2 bl.spamcop.net*1, postscreen_dnsbl_action=enforce
2. Анти-relay: smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination
3. Greylisting в Rspamd: timeout=5min, expire=1d, whitelist_symbols для прошедших DKIM/SPF — крупных провайдеров не задерживаем
4. TLS: smtpd_tls_security_level=may, smtpd_tls_protocols=">=TLSv1.2", сертификат Let's Encrypt с автопродлением certbot
5. Rate-limit через anvil: smtpd_client_message_rate_limit=100 при anvil_rate_time_unit=60s — гасим скомпрометированный ящик

РЕЗУЛЬТАТ

postscreen отсекает ботнеты ещё до SMTP-очереди, greylisting снимает основную массу спама без сигнатур; полезная нагрузка на Rspamd и ClamAV падает в разы

КЛЮЧЕВОЙ НЮАНС

milter_default_action=accept обязателен: при падении rspamd_proxy почта продолжает ходить без фильтра, а не встаёт колом — отказ фильтра не должен быть отказом почты

РЕАЛИЗАЦИЯ 3 ИЗ 3

Мониторинг доставляемости и репутации

Что настраиваем

Кабинеты постмастеров + разбор DMARC-отчётов + контроль RBL и PTR по всем доменам клиента

Как мы это делаем

1. PTR/FCrDNS: dig -x <IP> возвращает mail.domain, прямая A-запись ведёт обратно на IP; настраивается у хостера, не у регистратора
2. Google Postmaster Tools + Mail.ru Postmaster: еженедельный контроль spam rate (<0.1 %) и репутации домена
3. rua-отчёты DMARC собираем на выделенный ящик и разбираем parsedmarc'ом — сырой XML руками не читаем
4. Cron-проверка IP по zen.spamhaus.org и b.barracudacentral.org; при листинге — сначала устранение причины, потом делистинг

РЕЗУЛЬТАТ

Деградация репутации видна за дни до жалоб пользователей: аномальный spam rate или новый источник в DMARC-отчёте — сигнал к разбору, а не постфактум-аврал

КЛЮЧЕВОЙ НЮАНС

PTR правится в панели хостинг-провайдера (rDNS меняет владелец IP); запись у DNS-регистратора домена на обратную зону не влияет — частая точка путаницы

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Сразу -all в SPF**
  Забытые источники (CRM, 1С, сайт) начинают резаться у получателей. Стартуем с ~all, две недели читаем DMARC-отчёты, потом ужесточаем
- ✕ **Больше 10 DNS-lookups в SPF**
  Вложенные include облачных сервисов съедают лимит — permerror. Разворачиваем include в ip4:-блоки и пересчитываем механизмы
- ✕ **DKIM-ключ 1024 бита**
  У rspamadm dkim_keygen дефолт 1024; часть получателей считает такой ключ слабым. Всегда явно задаём -b 2048 (RFC 8301)
- ✕ **PTR указывает на хостера**
  rDNS вида v12345.hosting.ru роняет доверие Gmail/Mail.ru. Ставим mail.domain и проверяем совпадение прямой и обратной записи
- ✕ **milter_default_action=reject**
  Падение rspamd_proxy превращается в отказ всей почты. Держим accept и мониторим порт 11332 отдельной проверкой
- ✕ **p=reject без учёта форвардов**
  Пересылки и списки рассылки ломают SPF-alignment. Проверяем adkim/aspf=r и долю fail в rua-отчётах перед ужесточением политики
- ✕ **Greylisting задерживает всё подряд**
  Коды 2FA и уведомления опаздывают на 5 минут. Спасают whitelist_symbols по пройденным DKIM/SPF и белый список крупных провайдеров
- ✕ **Вечный DKIM-селектор**
  Один ключ годами — утечку не заметить. Ротируем селектор ежегодно (2026 → 2027): публикуем новый ключ, старую запись после перехода удаляем

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- SPF с ~all и переходом на -all после 2 недель мониторинга
- DKIM 2048 бит через Rspamd на все исходящие домены
- PTR = mail.domain + совпадение прямой и обратной записи
- TLS 1.2+ на smtpd/smtp, сертификат Let's Encrypt

НОРМАЛЬНО

- DMARC p=quarantine с rua-отчётами и еженедельным разбором
- postscreen с весами RBL (threshold=2) + greylisting в Rspamd
- Регистрация в Google Postmaster и Mail.ru Postmaster
- Rate-limit исходящих и алерт на всплеск очереди Postfix

ХОРОШО

- DMARC p=reject, ежегодная ротация DKIM-селектора
- MTA-STS и TLS-RPT для принудительного TLS на входящих
- Автопроверка RBL по cron с алертом в мониторинг
- parsedmarc + дашборд: динамика pass rate и источников отправки

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] SPF опубликован, механизмов не больше 10, и в нём есть ВСЕ источники: MX, CRM, 1С, сайт?
- [ ] DKIM-подпись 2048 бит стоит на каждом исходящем домене, селектор ротируется ежегодно?
- [ ] DMARC доведён до p=quarantine/reject, а rua-отчёты кто-то реально читает?
- [ ] PTR возвращает mail.domain, и прямая A-запись ведёт обратно на тот же IP?
- [ ] Spam rate в Google Postmaster ниже 0.1 %, репутация домена — High?
- [ ] Postfix не открытый relay: reject_unauth_destination проверен снаружи?
- [ ] IP сервера проверяется по RBL автоматически, а не после жалоб контрагентов?
- [ ] При падении антиспам-фильтра почта продолжит ходить (milter_default_action=accept)?

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).

- Аудит доставляемости за 1 день: SPF/DKIM/DMARC/PTR, репутация IP, тест реальными провайдерами, письменный отчёт
- Развёртывание Postfix + Dovecot + Rspamd под ключ с аутентификацией домена и мониторингом
- Вытаскиваем домен из спама: делистинг RBL, донастройка DNS, вывод spam rate в норму
- Сопровождение: еженедельный контроль постмастер-метрик, ротация ключей, обновления Postfix/Rspamd

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 — 3.11)

02 Postfix Postscreen Howto (postfix.org — 3.11)

03 Rspamd: модули DKIM Signing и Greylisting (docs.rspamd.com — 4.1)

04 RFC 7208 (SPF), RFC 6376 (DKIM), RFC 7489 (DMARC), RFC 8301 (DKIM-ключи) (rfc-editor.org — IETF)

05 RFC 8461 (MTA-STS), RFC 8460 (TLS-RPT) (rfc-editor.org — IETF)

06 Email Sender Guidelines (требования Google к отправителям) (support.google.com — 2026)

07 Наш шаблон main.cf + dkim_signing.conf для 10–50 PM (itfresh.ru — v2026)

Основано на официальной документации продуктов и нашей практике внедрения.