Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

SPF, DKIM, DMARC и BIMI: доставляемость под контролем

Как мы доводим домен клиента до DMARC p=reject и логотипа BIMI, не потеряв ни одного письма

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Письма компании уходят в спам, а от её домена рассылают фишинг: получатель не отличает ваш счёт от подделки. Мы приводим домен к жёсткой схеме — SPF в пределах 10 DNS-запросов, DKIM 2048 бит с rsa-sha256 на каждом источнике, DMARC по RFC 9989 от p=none к p=reject через разбор rua-отчётов, и только потом BIMI. Без этого канал деловой переписки работает вполсилы.

Почему это важно бизнесу

- Счёт или коммерческое предложение в папке «Спам» — это не ИТ-инцидент, а сорванная оплата и потерянная сделка.
- Фишинг от имени вашего домена бьёт по контрагентам: платёж уходит мошеннику, а объясняться придётся вам.
- От 5000 писем в сутки Gmail считает домен массовым отправителем: без SPF, DKIM и DMARC такая почта отбивается на входе.
- Репутация домена теряется за недели, а восстанавливается месяцами аккуратного прогрева трафика.
- Логотип BIMI в списке писем — узнаваемость отправителя и меньше шансов, что клиент откроет подделку.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

10

Предел DNS-запросов при вычислении SPF: превысили — permerror и провал проверки

RFC 7208, разд. 4.6.4

2048 бит

Длина RSA-ключа DKIM: по RFC 8301 минимум 1024, наш стандарт — 2048 и rsa-sha256

RFC 8301 и RFC 6376

RFC 9989

Стандарт DMARC с мая 2026: заменил RFC 7489, убрал pct, rf, ri, добавил np, psd и t

IETF: RFC 9989, 9990, 9991, 05.2026

4 недели

Наблюдение в p=none с rua до первого ужесточения: столько копим список отправителей

наш стандарт внедрения

32 КБ

Потолок файла логотипа BIMI: профиль SVG P/S, квадрат, обязательный элемент title

BIMI: профиль SVG Portable/Secure

0,1 / 0,3 %

Доля жалоб на спам в Gmail: цель — ниже 0,1 %, с 0,3 % начинается жёсткая фильтрация

Gmail: требования к отправителям

РЕАЛИЗАЦИЯ 1 ИЗ 3

SPF и DKIM: инвентарь отправителей и подпись на шлюзе

Что настраиваем

Все источники почты домена: Postfix и Rspamd, облачная почта, CRM, 1С, МФУ, сервис рассылок

Как мы это делаем

1. Собираем полный список отправителей: MX, заголовки Received, логи Postfix, интеграции 1С и CRM — из этого строим единственную TXT-запись v=spf1.
2. Считаем DNS-lookup: include, a, mx, ptr, exists и redirect тратят лимит из 10, пустых ответов допустимо два; редкие сервисы уносим на поддомен рассылок.
3. Подпись — Rspamd 4.1, модуль dkim_signing: свой selector, path /var/lib/rspamd/dkim/$domain.$selector.key, allow_hdrfrom_mismatch false, use_esld true.
4. В sign_headers оставляем оверподпись (o)from и (o)to: заголовок нельзя подставить повторно, не сломав подпись. Ключ — 2048 бит, алгоритм rsa-sha256.
5. Публикуем ключ в selector._domainkey TXT: v=DKIM1; k=rsa; p=... — строку бьём на части по 255 байт внутри одной записи, иначе зона не отдаётся.

РЕЗУЛЬТАТ

У домена ровно один валидный SPF без permerror и стабильная подпись со всех точек отправки. На стороне получателя в Authentication-Results видим spf=pass и dkim=pass, а доставка перестаёт зависеть от репутации одного IP-адреса.

КЛЮЧЕВОЙ НЮАНС

SPF привязан к конверту (MAIL FROM), а DMARC выравнивает домен из заголовка From. Сервис рассылок со своим bounce-доменом пройдёт SPF, но провалит alignment — спасает только DKIM ключом клиента.

РЕАЛИЗАЦИЯ 2 ИЗ 3

DMARC: путь от p=none к p=reject по данным rua

Что настраиваем

Основной домен и поддомены отправки: запись в _dmarc, сбор и разбор rua на своём parsedmarc с дашбордом

Как мы это делаем

1. Публикуем стартовую запись: v=DMARC1; p=none; rua=mailto:dmarc@домен; adkim=r; aspf=r — теги pct, rf и ri по RFC 9989 отменены и больше не пишутся.
2. Поднимаем parsedmarc 10.4: забор rua из отдельного ящика по IMAP, вывод в OpenSearch и дашборд Grafana по источникам и доле проходящих писем.
3. Четыре недели читаем отчёты: свои источники с fail — 1С, сканеры МФУ, старые CRM — достраиваем им SPF и DKIM, а не ослабляем политику домена.
4. Переводим на p=quarantine, две недели наблюдаем, затем p=reject; сразу задаём sp=reject и np=reject — поддомены и несуществующие имена закрыты.
5. Пересылку и рассылочные списки закрываем ARC по RFC 8617: на приёме проверяем цепочку ARC-Seal, чтобы легитимный форвард не отбивался по DMARC.

РЕЗУЛЬТАТ

Домен нельзя использовать для фишинга: письма без валидного выравнивания отклоняются на стороне получателя. Мы видим в дашборде каждый источник, объём и долю прохождения, а новый интегратор проявляется в отчётах в течение суток.

КЛЮЧЕВОЙ НЮАНС

Между quarantine и reject смотрим не общий процент прохождения, а поимённый список источников: забытый терминальный сервер с 1С даёт единицы писем в сутки и в проценте не виден.

РЕАЛИЗАЦИЯ 3 ИЗ 3

BIMI: сертификат, профиль SVG P/S и запись default._bimi

Что настраиваем

Домены с DMARC не ниже quarantine: логотип на HTTPS-хостинге, VMC под товарный знак либо CMC

Как мы это делаем

1. Проверяем предусловие: DMARC у домена из From и у организационного домена не ниже p=quarantine и без t=y — при p=none логотип не покажет ни один клиент.
2. Логотип готовим в профиле SVG P/S: baseProfile="tiny-ps", элемент title с названием, квадрат, сплошной непрозрачный фон, без растра, скриптов и ссылок наружу.
3. Под Gmail и Apple нужен VMC на зарегистрированный товарный знак, без регистрации выпускаем CMC; Yahoo и Fastmail принимают и самозаявленный логотип без сертификата.
4. Публикуем запись default._bimi TXT: v=BIMI1; l=https://.../logo.svg; a=https://.../vmc.pem — оба URL должны отдаваться по HTTPS напрямую, без редиректов.
5. Ставим на мониторинг срок действия сертификата и доступность ссылок l= и a=: просроченный VMC гасит логотип молча, без единой ошибки в почтовых логах.

РЕЗУЛЬТАТ

Письма компании отображаются с логотипом в поддерживающих клиентах, а сам факт отображения работает для получателя как визуальный признак подлинности. Побочный эффект полезен: жёсткий DMARC становится обязательным и его уже нельзя откатить незаметно.

КЛЮЧЕВОЙ НЮАНС

BIMI не заменяет аутентификацию и сам по себе доставляемость не улучшает: это витрина поверх уже жёсткого DMARC. Начинать с логотипа, не закрыв SPF и DKIM, бессмысленно.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

✕ Две записи SPF на одном домене

Провайдер и подрядчик добавляют по своей TXT — по RFC 7208 это permerror. Сводим в одну строку и закрываем правки DNS в обход администратора.

✕ Перебор лимита в 10 DNS-запросов

Каждый новый include съедает лимит, и проверка ломается молча. Считаем lookup при каждой правке, редкие сервисы выносим на поддомен рассылок.

✕ Ключ DKIM 1024 бит и rsa-sha1

По RFC 8301 rsa-sha1 применять нельзя, ключ короче 1024 бит верификатор считает невалидным. Перевыпускаем 2048 бит с rsa-sha256 на новом селекторе.

✕ TXT-ключ не разбит по 255 байт

Одна строка в TXT ограничена 255 байтами, а 2048-битный ключ длиннее. Панель DNS режет запись — публикуем двумя строками внутри одной TXT.

✕ Сразу p=reject, без периода отчётов

Без месяца rua теряются 1С, МФУ и забытые сервисы. Всегда сначала p=none со сбором отчётов, ужесточение — только по закрытому списку источников.

✕ Забытые теги sp и np

Политика основного домена не закрывает поддомены и несуществующие имена — фишинг уходит с news.домен. Ставим sp=reject и np=reject явно.

✕ SPF pass путают с alignment

Сервис рассылок проходит SPF по своему bounce-домену, но From чужой, и DMARC даёт fail. Лечится только подписью DKIM ключом самого клиента.

✕ Логотип BIMI в обычном SVG

Экспорт из редактора тянет скрипты, растр и внешние ссылки — валидатор отклоняет файл. Нужен baseProfile="tiny-ps", квадрат, до 32 КБ.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Одна TXT-запись SPF на домен, lookup посчитаны, хвост ~all на старте
- DKIM 2048 бит с rsa-sha256 на каждом источнике отправки писем
- DMARC p=none с рабочим ящиком rua и еженедельным разбором отчётов
- Перечень всех сервисов, отправляющих почту от имени домена, зафиксирован

НОРМАЛЬНО

- Разбор rua автоматом: parsedmarc 10.4 с дашбордом вместо чтения XML руками
- p=quarantine с заданными sp и np, хвост SPF переведён в -all
- Отдельный поддомен для массовых рассылок со своим SPF и DKIM
- Ротация DKIM-селекторов раз в год двумя ключами, без простоя подписи

ХОРОШО

- DMARC p=reject на домене и всех поддоменах, np=reject явным тегом
- ARC по RFC 8617 на приёме, чтобы пересылка и списки не отбивались
- MTA-STS (RFC 8461) и TLS-RPT (RFC 8460) поверх аутентификации отправителя
- BIMI с действующим VMC или CMC и контролем срока в мониторинге

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Знаем ли мы полный список сервисов, которые отправляют письма от имени нашего домена?
- [ ] SPF-запись одна, укладывается в 10 DNS-запросов и не даёт permerror при проверке?
- [ ] Все источники подписывают письма DKIM, а не только основной почтовый сервер?
- [ ] Настроен ли DMARC и приходят ли rua-отчёты в ящик, который кто-то реально читает?
- [ ] Заданы ли sp и np, чтобы поддомены и несуществующие имена нельзя было использовать?
- [ ] Есть ли план перехода на p=reject со сроками, а не бессрочный режим p=none?
- [ ] Ротируются ли DKIM-ключи и знаем ли мы, какой селектор активен прямо сейчас?
- [ ] Идут ли массовые рассылки с List-Unsubscribe и одним кликом отписки по RFC 8058?
- [ ] Мониторим ли мы наличие и содержимое TXT-записей SPF, DKIM и DMARC автоматически?
- [ ] Если внедрён BIMI — контролируется ли срок VMC и доступность файла логотипа?

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: инвентарь отправителей, разбор SPF, DKIM, DMARC и письменный план
- Настройка подписи на своём сервере: Postfix и Rspamd, ключи, селекторы, ротация
- Разворачиваем parsedmarc 10.4 с дашбордом и ведём домен от p=none до p=reject
- Подключаем BIMI: подготовка SVG P/S, выпуск VMC или CMC, публикация записи
- Ставим на мониторинг DNS-записи почты и срок действия сертификата BIMI

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 RFC 9989, 9990, 9991. DMARC: протокол и формат отчётов (rfc-editor.org — 2026)

02 RFC 7208. SPF, разд. 4.6.4: лимиты DNS-запросов (rfc-editor.org — 2014)

03 RFC 6376 и RFC 8301. DKIM: подпись, алгоритмы, длина ключа (rfc-editor.org — 2011/2018)

04 RFC 8617 ARC, RFC 8461 MTA-STS, RFC 8460 TLS-RPT (rfc-editor.org — 2018/2019)

05 BIMI: draft-brand-indicators-for-message-identification (datatracker.ietf.org — draft-12)

06 Rspamd: модуль dkim_signing и DKIM Signing Guide (docs.rspamd.com — 4.1)

07 parsedmarc: разбор rua, вывод в OpenSearch и Grafana (domainaware.github.io — 10.4)

08 Наш чек-лист внедрения DMARC и шаблоны DNS-записей (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.