Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DKIM, SPF и DMARC: аутентификация почтового домена

Как мы за час поднимаем три записи и за 4 недели доводим домен до p=reject

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Почта клиента формально работает, но коммерческие предложения, счета из 1С и уведомления CRM оседают в спаме, а от имени домена кто угодно может отправить письмо с From: директора. Домен без SPF, DKIM и DMARC приёмник не отличает от подделки. Итог — сорванные сделки, оплата по фальшивым реквизитам и разбор с контрагентами вместо работы.

Почему это важно бизнесу

- Письма в спаме = неотвеченные КП и просроченные счета: менеджер уверен, что отправил, клиент письма не видел
- Подделка From: директора или бухгалтера — прямой канал для платежа по чужим реквизитам
- Gmail отбивает неаутентифицированную рассылку ответом 550-5.7.26, а не кладёт её в спам: письма не доходят молча
- Испорченная репутация домена восстанавливается неделями прогрева, а не одной правкой DNS
- Один час работ в DNS против месяцев необъяснимой «тишины» на стороне клиентов

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

RFC 9989

DMARC-стандарт с мая 2026 вместо RFC 7489: pct, rf, ri в historic, рабочие теги t= и np=

RFC 9989, реестр тегов IANA

10 / 2

Лимит DNS-запросов и void-ответов в SPF: превышение любого из них даёт permerror

RFC 7208, разд. 4.6.4

2048 бит

Ключ DKIM: RFC 8301 требует минимум 1024 и рекомендует 2048 — 2048 наш стандарт

RFC 8301, разд. 3.2

28 дней

Наблюдение rua-отчётов до ужесточения: 14 дней на p=none и 14 на p=quarantine

регламент ITfresh

0,1%

Потолок доли жалоб на спам у Gmail; от 0,3% доставка проседает резко

Google, Email sender guidelines

604800 с

max_age MTA-STS: неделя кеша политики; потолок по стандарту — 31557600 секунд

RFC 8461, разд. 3.2

РЕАЛИЗАЦИЯ 1 ИЗ 3

Инвентаризация отправителей и одна SPF-запись

Что настраиваем

Домен клиента на 10-40 ящиков: почтовый узел, 1С, CRM, сервис рассылок, МФУ и система мониторинга — всё, что шлёт от имени домена

Как мы это делаем

1. Снимаем зону: dig +short TXT domain.ru, dig TXT _dmarc.domain.ru, dig TXT sel._domainkey.domain.ru — фиксируем дубли v=spf1 и мусор от прежних хостингов
2. Собираем реестр отправителей: MX и веб-почта, сервер 1С (SMTP 465/587), CRM, рассылочный сервис, сканы с МФУ, алерты Zabbix — include берём из доки каждого
3. Собираем ОДНУ TXT: v=spf1 ip4:<адрес> include:<сервис> ~all; считаем DNS-lookup рекурсивно и держим не более 7 из 10, механизм ptr не используем
4. Лишние источники уводим на отдельный поддомен-отправитель (mail. или crm.) со своим SPF, чтобы корневая запись не разбухала до permerror
5. Проверяем отсутствие include на несуществующие домены (void-лимит 2 по RFC 7208) и на время работ снижаем TTL записей до 300 секунд

РЕЗУЛЬТАТ

Одна валидная SPF-запись вместо двух-трёх конфликтующих, все реальные отправители авторизованы. Приёмники перестают выдавать permerror, и письма от 1С, CRM и рассылочного сервиса проходят проверку наравне с почтой основного сервера.

КЛЮЧЕВОЙ НЮАНС

Считаем lookup не по своей строке, а рекурсивно: чужой include внутри тянет ещё 5-6 запросов и молча выводит домен за лимит 10 — тогда SPF падает в permerror сразу у всех отправителей.

РЕАЛИЗАЦИЯ 2 ИЗ 3

DKIM: ключи, селекторы, ротация без простоя

Что настраиваем

Почтовый узел клиента — mailcow/Rspamd или Postfix + OpenDKIM, плюс облачные Яндекс 360 и Google Workspace на том же домене

Как мы это делаем

1. Генерируем пару 2048 бит: в mailcow — в карточке домена веб-интерфейса (ключи лежат в Redis), на Postfix — opendkim-genkey -b 2048 -s <селектор> -d domain.ru
2. Селектор кодируем датой ротации: itf2608._domainkey.domain.ru — вторая пара живёт рядом с первой, переключение идёт без окна простоя
3. Публикуем TXT v=DKIM1; k=rsa; h=sha256; p=… — в зонах с ограничением строки 255 символов ключ разбиваем на части внутри одной записи
4. В Rspamd dkim_signing ставим check_pubkey = true и allow_pubkey_mismatch = false (по умолчанию false и true): узел сам ловит расхождение ключа с DNS
5. Отдельный селектор каждому отправителю: Яндекс 360 — mail, Google Workspace — google (Gmail → Authenticate email, 2048 бит), рассылочному сервису — свой

РЕЗУЛЬТАТ

Каждое исходящее письмо несёт rsa-sha256-подпись, которую приёмник проверяет по DNS. DKIM переживает пересылку и смену IP, в отличие от SPF, поэтому именно он держит DMARC-выравнивание при форвардах и отправке через шлюзы.

КЛЮЧЕВОЙ НЮАНС

rsa-sha1 запрещён RFC 8301 к подписи и проверке, 1024 бит — нижняя граница, а не рабочее значение. Ed25519 по RFC 8463 публикуем только вторым ключом: крупные приёмники проверяют его ещё не повсеместно.

РЕАЛИЗАЦИЯ 3 ИЗ 3

DMARC: от p=none к p=reject по агрегатным отчётам

Что настраиваем

Корневой домен и все поддомены, с которых уходит почта; агрегатные rua-отчёты собираем в отдельный ящик и разбираем парсером

Как мы это делаем

1. Стартуем с v=DMARC1; p=none; rua=mailto:dmarc@domain.ru; fo=1 — блокировок нет, но приёмники начинают слать суточные XML-отчёты
2. Две недели разбираем rua: источники с spf=fail/dkim=fail делим на свои забытые системы и чужие подделки, свои — вносим в SPF и подписываем DKIM
3. Ужесточаем до p=quarantine ещё на две недели; если поток рискованный, ставим p=reject; t=y — по RFC 9989 тег t=y понижает применяемую политику на ступень
4. Финал: p=reject; sp=reject; np=reject; adkim=s; aspf=s, тег t снимаем — строгое выравнивание плюс отдельная политика для несуществующих поддоменов
5. Закрываем транспорт: политика MTA-STS на mta-sts.domain.ru с mode: enforce и max_age: 604800, плюс TXT _smtp._tls со строкой v=TLSRPTv1 для TLS-RPT

РЕЗУЛЬТАТ

Подделать From: домена клиента с чужого сервера больше нельзя — письмо отклоняется на стороне приёмника. Поддомены, которых нет в DNS, закрыты тегом np=reject, причём RFC 9989 ищет политику обходом дерева DNS вверх, без Public Suffix List.

КЛЮЧЕВОЙ НЮАНС

p=reject без месяца отчётов = блокировка своих же счетов из 1С и уведомлений CRM. Обратная крайность — вечный p=none: это диагностика, а не защита. И t=y не защита: он снижает политику на ступень.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Две записи v=spf1 на одном домене**
  Осталась от прежнего хостинга. По RFC 7208 это permerror, часть приёмников отбрасывает обе. Лечим объединением в одну строку, лишнюю удаляем.

- ✕ **Превышен лимит 10 DNS-запросов**
  Каждый include рекурсивно тянет свои. Считаем дерево целиком, лишние источники выносим на поддомен, механизмы ptr и избыточные a/mx убираем.

- ✕ **Жёсткий -all до инвентаризации**
  Отрубает 1С, CRM и МФУ, о которых никто не вспомнил. Идём ~all, месяц читаем rua-отчёты и только потом ставим -all, когда реестр закрыт.

- ✕ **DKIM только на основном домене**
  Поддомены и вторые домены шлют письма без подписи. Отдельная пара ключей и своя TXT нужны каждому реально отправляющему домену и поддомену.

- ✕ **pct=10 в новой записи DMARC**
  В RFC 9989 тег переведён в historic вместе с rf и ri, приёмники его игнорируют — политика применяется целиком. Плавный ввод теперь только через t=.

- ✕ **p=quarantine; t=y как рабочий режим**
  t=y понижает применяемую политику ровно на ступень, то есть quarantine превращается в none. Тестовый тег снимаем сразу после проверки потока.

- ✕ **Забыли PTR и HELO**
  Обратная запись и имя в HELO должны совпадать с FQDN узла. Иначе Exchange и Outlook.com штрафуют письмо даже при pass по SPF, DKIM и DMARC.

- ✕ **Ключ DKIM не менялся годами**
  Утёкший приватный ключ подписывает что угодно от имени домена. Селектор с датой плюс ротация раз в 6-12 месяцев закрывают это без простоя.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Одна SPF-запись со всеми отправителями и мягким ~all на старте
- DKIM RSA-2048 с алгоритмом rsa-sha256 на основном домене
- DMARC v=DMARC1; p=none; rua=mailto:… и живой ящик для отчётов
- PTR для IP почтового узла, HELO = FQDN сервера

НОРМАЛЬНО

- DKIM на всех отправляющих доменах и поддоменах, селектор с датой
- p=quarantine после двух недель разбора rua; страховка — p=reject; t=y
- SPF не более 7 DNS-lookup из 10, лишние источники — на поддомен
- Парсер агрегатных отчётов и ежемесячная сводка по источникам

ХОРОШО

- p=reject; sp=reject; np=reject; adkim=s; aspf=s на всех доменах
- MTA-STS mode: enforce, max_age 604800 и TXT _smtp._tls с v=TLSRPTv1
- ARC-подпись на шлюзе, ротация ключей DKIM раз в полгода
- Еженедельная сверка Postmaster Tools, Яндекс Постмастера и DNSBL

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] В зоне домена ровно одна TXT-запись v=spf1 — проверено через dig, а не по памяти админа?
- [ ] Все системы, шлющие от имени домена (1С, CRM, рассылки, МФУ, мониторинг), внесены в реестр отправителей?
- [ ] Рекурсивное число DNS-lookup в SPF посчитано и укладывается в лимит 10 по RFC 7208?
- [ ] DKIM настроен на каждом домене и поддомене, с которого реально уходит почта?
- [ ] Длина ключа DKIM 2048 бит, алгоритм rsa-sha256, rsa-sha1 нигде не используется?
- [ ] Есть запись _dmarc и живой ящик rua, отчёты кто-то реально читает еженедельно?
- [ ] В записи DMARC нет тегов pct, rf, ri, а тест сделан через t= с учётом понижения на ступень?
- [ ] Политика для поддоменов задана явно тегами sp= и np=, а не унаследована по умолчанию?
- [ ] PTR-запись для IP почтового узла настроена провайдером и совпадает с именем в HELO?
- [ ] Ключи DKIM ротируются по расписанию, а схема селекторов позволяет менять их без простоя?

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 зоны и почтового узла: снимок SPF/DKIM/DMARC, PTR, HELO, проверка IP по DNSBL
- Сборка одной SPF-записи, генерация и публикация DKIM-ключей 2048 бит на всех доменах
- Сопровождение перехода p=none → quarantine → reject по агрегатным отчётам, 4-6 недель
- Настройка MTA-STS и TLS-RPT, ежемесячная сводка по источникам и доле жалоб
- Регламент ротации DKIM-ключей и приём домена под наш мониторинг доставляемости

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 — DMARC: теги p, sp, np, t, adkim, aspf, DNS tree walk (rfc-editor.org — 2026)

02 RFC 9990 и RFC 9991 — агрегатные и failure-отчёты DMARC (rfc-editor.org — 2026)

03 RFC 7208 — SPF: механизмы, лимит 10 lookup, void-лимит 2 (rfc-editor.org — 2014)

04 RFC 6376 и RFC 8301 — DKIM, rsa-sha256, длина ключей (rfc-editor.org — 2011/2018)

05 RFC 8461 и RFC 8460 — MTA-STS и TLS-RPT (rfc-editor.org — 2018)

06 Rspamd: модуль dkim_signing (check_pubkey, selector_map) (docs.rspamd.com — 4.x)

07 mailcow: DNS setup, DKIM и ARC в веб-интерфейсе (docs.mailcow.email — 2026)

08 Google Workspace Admin Help: Email sender guidelines, DKIM (support.google.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.