Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DMARC в корпоративной почте: путь от p=none до p=reject

Наша методика: отчёты RUA, alignment сторонних отправителей, MTA-STS, TLS-RPT, BIMI

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Домен подделывают без доступа к серверам клиента: письмо с чужого узла уходит контрагенту от имени директора, и в логах нашей почты его нет. Параллельно легитимные письма из 1С, CRM и рассылок оседают в спаме. Мы закрываем обе задачи одним контуром: аутентификация всех источников, выравнивание доменов по DKIM и SPF, управляемый переход политики DMARC к reject.

Почему это важно бизнесу

- Подделка поля From — это платёжка контрагенту с чужими реквизитами: деньги уходят раньше, чем кто-то заметит подмену.
- Счета и акты из 1С в спаме — сорванные сроки оплаты и разбор «мы ничего от вас не получали».
- Крупные приёмники требуют от массовых отправителей SPF, DKIM, DMARC и отписку в один клик — иначе письма не доходят.
- Домен без политики втягивают в чужие фишинговые кампании, а репутацию отправителя потом восстанавливают месяцами.
- Без отчётов RUA компания не знает, кто и с каких IP шлёт письма от её имени прямо сейчас.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

RFC 9989

Действующая редакция DMARC: обсолетит RFC 7489 и 9091, по ней пишем записи _dmarc

RFC 9989, май 2026

10 + 2

Лимит SPF: DNS-запросов механизмов и void-запросов, превышение даёт permerror

RFC 7208, раздел 4.6.4

2048 бит

Длина RSA-ключа DKIM при подписи; rsa-sha1 запрещён, ключ меньше 1024 бит невалиден

RFC 8301

0,10 %

Целевая доля жалоб на спам у массового отправителя, 0,30 % — жёсткий потолок

Google Email sender guidelines

31557600

Потолок max_age в MTA-STS; в enforce ставим 1209600 — две недели кэша политики

RFC 8461

30 дней

Держим прежний DKIM-селектор в DNS после ротации, пока не отойдут отложенные письма

наш регламент ротации ключей

РЕАЛИЗАЦИЯ 1 ИЗ 3

Инвентаризация отправителей: конвейер разбора RUA

Что настраиваем

Основной домен и поддомены клиента, выделенная VM со стеком parsedmarc 10.4 + OpenSearch + Grafana и ящиком для отчётов

Как мы это делаем

1. Публикуем _dmarc: v=DMARC1; p=none; rua=mailto:…; ruf=mailto:…; fo=1 — режим наблюдения, доставка писем не меняется
2. Ящики отчётов выносим на отдельный домен: там публикуем <наш-домен>._report._dmarc с v=DMARC1, иначе приёмник отчёты не пришлёт
3. parsedmarc забирает отчёты по IMAP или Microsoft Graph, пишет индекс на каждый день и отдаёт дашборд по source_ip и alignment
4. Две-три недели сводим таблицу: IP → сервис → есть ли подпись нашим доменом → попадает ли в SPF. Так находим формы сайта, мониторинг, банк-клиент
5. Каждый найденный источник получает include в SPF, собственный DKIM-селектор либо запрет на отправку от имени домена

РЕЗУЛЬТАТ

На выходе — закрытый список легитимных отправителей и точная доля трафика, уже проходящего DMARC. Дальше политику двигаем не на глаз, а по этой доле; неопознанный поток виден по адресам и объёму задолго до включения enforcement.

КЛЮЧЕВОЙ НЮАНС

Failure-отчёты присылают единицы приёмников и с урезанными заголовками — разбор инцидентов планируем только на агрегированных отчётах. Хранение по дневным индексам упрощает чистку по сроку.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Выравнивание сторонних сервисов: CRM, 1С, рассылки

Что настраиваем

Транзакционные и массовые отправители: 1С через SMTP, CRM, формы сайта, сервис рассылок; поддомены-отправители и их Return-Path

Как мы это делаем

1. Каждому классу отправки выделяем поддомен: crm., news., bill. — своя SPF-запись, свой DKIM-селектор, своя политика sp и своя репутация
2. У сервиса рассылок включаем собственный домен: Return-Path переводим на bounce-поддомен, домен SPF выравнивается с From и aspf=r проходит
3. Публикуем ключ сервиса так, чтобы подпись шла нашим доменом; в Authentication-Results проверяем, что header.d совпадает с доменом From
4. Держимся в 10 DNS-запросах SPF: разносим include по поддоменам, часть узлов подключаем напрямую ip4/ip6, мёртвые include вычищаем
5. В массовые рассылки добавляем List-Unsubscribe с HTTPS-URI и List-Unsubscribe-Post: List-Unsubscribe=One-Click по RFC 8058

РЕЗУЛЬТАТ

Рассылки и транзакционные письма проходят DMARC по DKIM даже после пересылки, а просадка репутации маркетингового поддомена не тянет за собой корпоративную переписку. Массовые отправки отвечают требованиям крупных приёмников по аутентификации и отписке.

КЛЮЧЕВОЙ НЮАНС

Alignment ломается не на подписи, а на домене: подпись сервиса при нашем адресе в From даёт dkim=pass и одновременно DMARC fail. Смотрим не «есть ли DKIM», а совпадает ли header.d с доменом From.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Enforcement и транспорт: reject, MTA-STS, TLS-RPT, BIMI

Что настраиваем

Политика основного домена и поддоменов, TLS-контур приёма почты, брендирование в inbox после стабильного reject

Как мы это делаем

1. Из p=none идём в p=quarantine с t=y: тег pct в RFC 9989 удалён, мягкость даёт t=y — приёмник применяет политику на уровень ниже
2. Через две недели снимаем t=y, затем ставим p=reject; отдельно задаём sp для существующих поддоменов и np=reject для несуществующих
3. Поднимаем MTA-STS: TXT _mta-sts с v=STSv1 и id по дате правки, файл политики на mta-sts.<домен> по пути /.well-known/mta-sts.txt, mode=testing
4. Включаем _smtp._tls с v=TLSRPTv1 и rua, читаем JSON-отчёты о STARTTLS и сертификатах и только после чистых суток переводим MTA-STS в mode=enforce
5. BIMI подключаем последним: default._bimi с v=BIMI1, тегами l и a; логотип SVG Tiny P/S, квадрат, до 32 КБ; сертификат VMC или CMC

РЕЗУЛЬТАТ

Подделки отбиваются на стороне приёмника, а не копятся в спам-папках получателей. Downgrade STARTTLS закрыт политикой MTA-STS, проблемы TLS видны в отчётах раньше жалоб. Логотип в списке писем отличает нашу почту от имитаций.

КЛЮЧЕВОЙ НЮАНС

Идентификатор id в записи _mta-sts обязан меняться при каждой правке политики, иначе у приёмника до конца max_age живёт старый кэш. Смена MX без обновления файла политики в режиме enforce = отказ приёма.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

× **Две SPF-записи на одном домене**
Приёмник отдаёт permerror, и SPF не проходит вовсе. Держим одну TXT v=spf1, объединяя механизмы, и перепроверяем после каждой правки зоны.

× **pct=10 как «плавный ролаут»**
В RFC 9989 теги pct, rf и ri удалены. Плавность даёт t=y: политика объявлена, но приёмник применяет её на уровень мягче.

× **Жёсткий -all при активной пересылке**
SPF рвётся на форвардинге и списках рассылки. Опора — выравнивание по DKIM: подпись переживает пересылку, письмо остаётся валидным.

× **Подпись доменом стороннего сервиса**
dkim=pass есть, DMARC — fail: домены не выровнены. Требуем от сервиса подпись нашим доменом и собственный Return-Path.

× **Не задан np для поддоменов**
Подделку шлют с несуществующего поддомена, где политики нет. Ставим np=reject сразу, ещё на этапе p=none для основного домена.

× **rua на чужой домен без разрешения**
Без записи <наш-домен>._report._dmarc с v=DMARC1 на домене-приёмнике отчёты просто не приходят, а инвентаризация стоит на месте.

× **Ротация DKIM одним шагом**
Старый селектор сносят вместе с ключом — письма в очередях перестают проверяться. Новый публикуем заранее, старый снимаем через 30 дней.

× **Логотип BIMI обычным SVG**
Нужен профиль SVG Tiny P/S: квадрат, до 32 КБ, без скриптов и внешних ссылок, плюс VMC или CMC и политика не ниже quarantine.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Одна SPF-запись в пределах 10 DNS-запросов, DKIM rsa-sha256 от 2048 бит
- _dmarc с p=none и rua на выделенный ящик, разбор отчётов раз в неделю
- Полный список источников отправки: почта, 1С, CRM, сайт, мониторинг, банк
- PTR и обратная зона для каждого IP, с которого уходит корпоративная почта

НОРМАЛЬНО

- p=quarantine с t=y, затем p=reject; теги sp и np заданы явно
- parsedmarc 10.4 с дашбордом: доля aligned-трафика и разбивка по source_ip
- Отдельные поддомены и селекторы под рассылки, CRM и транзакционные письма
- Ротация DKIM-ключей раз в полгода с перекрытием двух селекторов

ХОРОШО

- MTA-STS в mode=enforce и TLS-RPT с регулярным разбором JSON-отчётов
- BIMI с сертификатом VMC или CMC после стабильного p=reject
- Мониторинг DNS-записей почты и срока сертификата с алертом в Telegram
- Ежеквартальный пересмотр SPF: снятие мёртвых include и void-запросов

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] SPF-запись на домене одна и укладывается в 10 DNS-запросов и 2 void-запроса?
- [ ] Все источники отправки от имени домена найдены, внесены в SPF и подписаны DKIM?
- [ ] Ключи DKIM от 2048 бит, алгоритм rsa-sha256, ротация с перекрытием регламентирована?
- [ ] У рассылок и CRM header.d подписи совпадает с доменом в поле From письма?
- [ ] Отчёты RUA приходят и разбираются, известна доля писем, проходящих DMARC?
- [ ] Заданы sp и np — политики для существующих и несуществующих поддоменов?
- [ ] Зафиксированы дата перехода на p=reject и ответственный за этот переход?
- [ ] Опубликованы MTA-STS и TLS-RPT, id политики меняется при каждой правке?
- [ ] В массовых рассылках есть List-Unsubscribe-Post с отпиской в один клик?
- [ ] Изменения почтовых DNS-записей отслеживает мониторинг, а не только человек?

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 DNS и заголовков: находим все системы, шлющие письма от имени домена
- Разворачиваем сбор и разбор отчётов RUA: parsedmarc, хранилище, дашборд
- Ведём домен от p=none до p=reject без потерь легитимной почты по пути
- Настраиваем DKIM на сервере и у сторонних сервисов с выравниванием доменов
- Внедряем MTA-STS, TLS-RPT и BIMI, ставим мониторинг записей и сертификатов

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 (DMARCbis): теги политики, alignment, tree walk (rfc-editor.org — 2026)

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

03 RFC 7208, 6376, 8301 — SPF и DKIM: лимиты, селекторы, алгоритмы (rfc-editor.org — 2011-2018)

04 RFC 8461 и RFC 8460 — MTA-STS и TLS-RPT: mode, max_age, отчёты (rfc-editor.org — 2018)

05 RFC 8058 — List-Unsubscribe-Post: отписка в один клик (rfc-editor.org — 2017)

06 Email sender guidelines — требования к отправителям почты (support.google.com — 2026)

07 BIMI Implementation Guide: SVG Tiny P/S, VMC и CMC (bimigroup.org — 2026)

08 DKIM signing module — селекторы, пути к ключам, ротация (docs.rspamd.com — 4.1)

Основано на официальной документации продуктов и нашей практике внедрения.