



команда роста на аутсорсе
для системного улучшения ключевых метрик

Чек-лист по технической настройке домена и прогреву для Email-рассылок

Пошаговое руководство для улучшения доставляемости и избежания спама

Подготовка домена

☐ Выбрать отдельный поддомен для рассылок

Например, `mail.вашдомен.ru` или `email.вашдомен.ru`. Это изолирует репутацию основного домена от возможных проблем с рассылками.

☐ Создать корпоративную почту на выбранном поддомене

Например, `info@mail.вашдомен.ru`. Использование бесплатных почтовых ящиков (@gmail.com, @yandex.ru) значительно повышает риск попадания в спам.

Настройка DNS-записей

Корректная настройка DNS-записей SPF, DKIM и DMARC критически важна для аутентификации ваших писем. Это подтверждает почтовым провайдерам, что вы являетесь законным отправителем, и помогает избежать попадания в спам. Внедряйте их в строгой последовательности: SPF, затем DKIM, и только потом DMARC (Deployteq).

SPF (Sender Policy Framework)

☐ Создать TXT-запись SPF

Эта запись указывает, каким почтовым серверам разрешено отправлять письма от имени вашего домена. Добавьте её в DNS-записи вашего поддомена.

☐ Пример синтаксиса SPF-записи

```
`v=spf1 include:_spf.google.com include:spf.mail.ru include:spf.unisender.com ~all`
```

- `v=spf1`: Указывает версию SPF.

- `include`: Разрешает отправку писем с серверов, указанных в SPF-записях других доменов (например, вашего ESP).

- `~all`: Мягкий отказ (softfail). Письма, отправленные с неавторизованных серверов, будут помечены, но не отклонены. Для начала рекомендуется использовать `~all`.

☐ Убедиться, что в DNS есть только одна SPF-запись для домена

Наличие нескольких SPF-записей может привести к ошибкам аутентификации.

DKIM (DomainKeys Identified Mail)

☐ Сгенерировать DKIM-ключ

Обычно это делается через панель управления вашего ESP (провайдера рассылок). Вы получите публичный ключ, который нужно добавить в DNS.

❑ Добавить TXT-запись DKIM

Запись будет иметь вид `селектор.\_domainkey.вашподдомен.ru` со значением, предоставленным вашим ESP.

Например:

`host: s1.\_domainkey.mail.вашдомен.ru`

`value: v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDy...`

❑ Проверить корректность DKIM-записи

Используйте онлайн-инструменты для проверки DNS-записей.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

❑ Настроить DMARC-политику

DMARC использует результаты SPF и DKIM для определения, как обрабатывать письма, не прошедшие аутентификацию. Добавьте TXT-запись для `\_dmarc.вашподдомен.ru`.

❑ Начальная DMARC-политика

`v=DMARC1; p=none; rua=mailto:your\_email@вашдомен.ru; ruf=mailto:your\_email@вашдомен.ru; fo=1`

- `v=DMARC1`: Версия DMARC.
- `p=none`: Политика 'none' (мониторинг). Письма не отклоняются, но вы получаете отчёты.
- `rua`: Адрес для агрегированных отчётов.
- `ruf`: Адрес для forensic-отчётов.
- `fo=1`: Генерировать forensic-отчёты, если хотя бы одна из проверок (SPF или DKIM) не прошла.

❑ Постепенный переход к более строгим политикам

После анализа отчётов DMARC и подтверждения корректности настроек, перейдите к `p=quarantine` (помещать в спам) или `p=reject` (отклонять письма), чтобы полностью защитить домен от спуфинга.

Инструменты для проверки DNS-записей

MXToolbox	Проверка SPF, DKIM, DMARC
DMARC Analyzer	Анализ DMARC-отчётов
Google Admin Toolbox (Check MX)	Общая проверка DNS-записей

Прогрев домена и IP-адреса

Прогрев домена — это постепенное увеличение объёма отправляемых писем с нового домена (или домена, который долго не использовался для рассылок) для формирования положительной репутации у почтовых провайдеров (Postmark). Этот процесс занимает 3-6 недель (Postmark) и помогает избежать попадания писем в спам.

Рекомендуемый график прогрева (пример)

Период	Объём отправки в день	Прирост	Комментарии
Дни 1-2	50-100 писем	Низкий	Отправляйте самым активным подписчикам, избегайте промо.
Дни 3-7	100-200 писем	Удваивайте	Если показатели вовлечённости нормальные (Postmark).

Период	Объём отправки в день	Прирост	Комментарии
Неделя 2	200-500 писем	20-50%	Продолжайте отправлять активной базе, следите за метриками.
Неделя 3	500-1000 писем	20-50%	Включайте более широкие сегменты активной базы.
Неделя 4	1000-2500 писем	20-50%	Можно начинать тестировать небольшие промо-рассылки.
Неделя 5+	2500-5000+ писем	20-50%	Постепенно выходите на целевой объём, продолжайте мониторинг.
Важно	Не увеличивайте объём, если видите проблемы с доставляемостью или жалобами (Postmark).		При проблемах снизьте объём на 25-30% (Postmark).

Рекомендации по контенту для первых писем

☐ Начинайте с приветственных писем

Приветственные серии имеют открываемость до 50-60% и помогают установить контакт (статья).

☐ Отправляйте полезный, некоммерческий контент

Информационные письма, полезные советы, гайды. Избегайте прямых продаж и агрессивных промо-предложений.

☐ Используйте активную и чистую базу

Отправляйте письма подписчикам, которые недавно взаимодействовали с вашим брендом или дали явное согласие на рассылку (Postmark).

Мониторинг и устранение проблем

☐ Использовать постмастеры почтовых провайдеров

Регулярно проверяйте репутацию домена и IP-адреса в Google Postmaster Tools и Яндекс.Постмастер.

☐ Отслеживать Bounce Rate

Норма — не выше 5%. Высокий Bounce Rate (процент недоставленных писем) указывает на проблемы с качеством базы или блокировку. Hard Bounce (несуществующий адрес) должен быть не более 1% (JustRelate). Soft Bounce (временные проблемы) требует внимания.

☐ Контролировать Spam Complaint Rate

Процент жалоб на спам должен быть минимальным, желательно не выше 0.1%. Превышение 0.3% может привести к блокировкам (JustRelate).

☐ Валидация базы адресов

Регулярно используйте сервисы валидации для очистки базы от неактивных и несуществующих адресов. Это снижает Bounce Rate и улучшает доставляемость.

Сервисы для валидации базы

ZeroBounce	Платный, высокая точность
Hunter.io Email Verifier	Платный, есть бесплатный лимит
Email Hippo	Платный

Глоссарий терминов

SPF (Sender Policy Framework)	DNS-запись, указывающая разрешённые почтовые серверы для отправки писем от имени домена.
DKIM (DomainKeys Identified Mail)	DNS-запись, добавляющая цифровую подпись к письмам для проверки их целостности и подлинности отправителя.
DMARC (Domain-based Message Authentication, Reporting & Conformance)	DNS-запись, определяющая политику обработки писем, не прошедших SPF и DKIM аутентификацию, и предоставляющая отчёты.
Bounce Rate	Процент писем, которые не были доставлены получателю.
Hard Bounce	Необратимая ошибка доставки (например, несуществующий адрес).
Soft Bounce	Временная ошибка доставки (например, переполненный ящик).

Ссылки на официальные руководства почтовых провайдеров

Google Postmaster Tools	https://postmaster.google.com/
Яндекс.Постмастер	https://postmaster.yandex.ru/
Microsoft Sender Support	https://sendersupport.olc.protection.outlook.com/

Больше интересного в нашем блоге

развивайте бизнес-мышление с нашими исследованиями



Получить пользу

