Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DNSSEC: подписание зоны и эксплуатация без SERVFAIL

Перевод зон на dnssec-policy, автоматика DS через CDS и честный мониторинг подписей

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Задача — закрыть подмену DNS-ответов для доменов клиента: почты, личных кабинетов, публикаций 1С, VPN-эндпоинтов. Без подписи зоны отравленный кэш уводит MX и A на чужой хост. Но неаккуратное включение ломает домен целиком: одна просроченная RRSIG или рассинхрон DS с родительской зоной — и валидирующие резолверы отдают SERVFAIL всем сразу.

Почему это важно бизнесу

- Подмена A/MX уводит почту и платёжные уведомления на чужой сервер: это не простой, а утечка переписки и деньги.
- Ошибка при включении даёт SERVFAIL всему домену: одновременно падают сайт, почта и веб-публикации 1С.
- Подписи истекают тихо: без мониторинга авария всплывает через час, когда звонят пользователи и контрагенты.
- Откат после SERVFAIL упирается в TTL DS и кэши резолверов: домен «лечится» часами, а не за одну правку.
- Ручной rollover ключей — плановое окно риска раз в квартал; автоматика убирает человеческий фактор.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

9.20

минимальная ветка BIND: 9.18 снят с поддержки в июне 2026, 9.20 живёт до 2028

ISC, политика поддержки веток BIND

P14D

signatures-validity встроенной policy default; обновление — signatures-refresh P5D

BIND 9.20, вывод named -C

0

единственное значение iterations для NSEC3, которое примет dnssec-policy

RFC 9276 и BIND 9.20 ARM

50

потолок итераций NSEC3 при валидации (было 150), выше — ответ считается insecure

BIND 9.20, release notes

1232

max-udp-size в BIND и edns-buffer-size в Unbound: значение по умолчанию у обоих

DNS Flag Day 2020, доки BIND и Unbound

15 мин

интервал наших проб AD-флага; порог алерта по остатку RRSIG — ниже signatures-refresh

регламент DNSSEC ITfresh

РЕАЛИЗАЦИЯ 1 ИЗ 3

Подписание зоны: BIND 9.20 на dnssec-policy

Что настраиваем

Две авторитативные NS клиента (primary + secondary), от 1 до 8 публичных зон, inline-signing на primary

Как мы это делаем

1. Ставим BIND 9.20 (ветка 9.18 снята с поддержки в июне 2026), на резолверах dnssec-validation auto, на NS — chrony: уход часов ломает inception/expiration подписей.
2. Политику пишем явно, а не built-in default (ISC меняет его между версиями): keys { csk lifetime unlimited algorithm ecdsa256; }, dnskey-ttl PT1H, purge-keys P90D.
3. Для NSEC3 — nsec3param iterations 0 optout no salt-length 0: iterations больше нуля dnssec-policy не примет (RFC 9276), optout включаем только на делегирующих зонах.
4. Применяем: named-checkconf, затем rndc reconfig; состояние ключей — rndc dnssec -status <zone>, подписи — dig @localhost <zone> DNSKEY +dnssec.
5. Отдаём secondary по AXFR/IXFR с TSIG hmac-sha256 и проверяем, что подписанная зона доехала: RRSIG на SOA, DNSKEY и NS.

РЕЗУЛЬТАТ

Зона подписана без остановки резолвинга: подписи и ротация ключей живут внутри named, ручных dnssec-signzone и cron-обвязки нет. Inline-signing в 9.20 включён по умолчанию, поэтому правки вносятся в обычный файл зоны, а named собирает подписанную копию в файл с расширением .signed.

КЛЮЧЕВОЙ НЮАНС

Мануалы с auto-dnssec maintain неприменимы: в 9.20 такого параметра уже нет, зона переносится на dnssec-policy целиком. Сверяемся с блоком dnssec-policy в ARM, а не с чужими howto.

РЕАЛИЗАЦИЯ 2 ИЗ 3

DS в родительской зоне: CDS/CDNSKEY вместо ручной вставки

Что настраиваем

Делегирование в .ru/.рф через панель регистратора плюс автоматика CDS на наших NS

Как мы это делаем

1. Публикуем CDS/CDNSKEY: в BIND их печатает сама policy (cdnskey yes, cds-digest-types — SHA-256), в PowerDNS 5.0 — pdnsutil zone set-publish-cds.
2. В блоке зоны задаём parental-agents (адреса NS родителя, лучше с TSIG) и checkds explicit — named сам опрашивает DS и доводит ключ до состояния omnipresent.
3. Регистратор не читает CDS — DS вносим руками (алгоритм 13, digest type 2) и подтверждаем вручную: rndc dnssec -checkds -key <id> published <zone>.
4. Окно ожидания считаем как parent-ds-ttl (по умолчанию P1D) плюс parent-propagation-delay (PT1H): пока старый DS в кэшах, старый KSK из зоны не убираем.
5. Контроль снаружи: delv +rtrace через валидатор, dig +dnssec на флаг ad и dig @<NS родителя> <zone> DS.

РЕЗУЛЬТАТ

Публикация DS перестаёт быть ручной операцией по памяти: смена KSK едет по цепочке CDS→DS без тикета регистратору, а PowerDNS 5.0 умеет и bootstrapping по RFC 9615. Где self-service не поддержан, процедура зафиксирована по шагам и с явным окном ожидания, поэтому rollover не даёт SERVFAIL.

КЛЮЧЕВОЙ НЮАНС

Главный риск rollover — снять старый ключ раньше, чем родительский DS вымоется из кэшей. Окно не сокращаем; в Knot DNS 3.4 ту же логику закрывают ksk-submission и cds-cdnskey-publish.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Эксплуатация: мониторинг подписей и валидация на резолверах

Что настраиваем

Все подписанные зоны клиента плюс внутренние резолверы в офисе и на терминальных серверах

Как мы это делаем

1. Проба каждые 15 минут: dig/kdig через два независимых валидирующих резолвера — ждём флаг ad; расхождение ответов между NS ловим отдельным чеком.
2. Считаем остаток жизни RRSIG по полю expiration у SOA и DNSKEY: warning при остатке меньше 3 суток, critical — меньше 24 часов.
3. Пороги держим ниже signatures-refresh (P5D): при default подписи штатно обновляются на пятые сутки, и алерт «меньше 7 суток» звонил бы каждый цикл.
4. Zabbix 7.0, агент 2: ключ net.dns.get по зоне и типу DNSKEY с флагами dnssec и adflag — в JSON видно AD и expiration; алерт в Telegram называет зону и ключ.
5. На резолверах: dnssec-validation auto (BIND) либо auto-trust-anchor-file с RFC 5011 (Unbound), val-log-level 2, aggressive-nsec и буфер 1232 не занижаем.

РЕЗУЛЬТАТ

Просроченные подписи и оборванная цепочка доверия перестают быть внезапным падением почты: мы узнаём о проблеме за сутки-трое до expiration и до того, как её увидят пользователи. Валидация на внутренних резолверах закрывает подмену ответов уже внутри периметра.

КЛЮЧЕВОЙ НЮАНС

Мониторить факт «сайт открывается» бесполезно: невалидирующий резолвер отдаст ответ и при битой подписи. Проверяем именно флаг ad и остаток жизни RRSIG, обязательно с двух разных резолверов.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Время на NS уехало**
  Подписи привязаны к inception/expiration: уход часов на десятки минут делает зону BOGUS. Держим chrony на всех NS и мониторим offset отдельной пробой.

- ✕ **Старый KSK сняли раньше DS**
  Валидаторы держат прежний DS весь TTL. Ключ снимаем после parent-ds-ttl плюс parent-propagation-delay и подтверждения rndc dnssec -checkds.

- ✕ **NSEC3 с большими iterations**
  Наследие старых howto: iterations 10+ и соль. BIND считает более 50 итераций insecure, а policy примет только 0. В PowerDNS — set-nsec3 '1 0 0 -'.

- ✕ **Ответы режутся на 512 байтах**
  DNSKEY и RRSIG не влезают в UDP без EDNS0. Значение 1232 у max-udp-size и edns-buffer-size не занижаем и проверяем, что TCP/53 не закрыт.

- ✕ **Secondary отдаёт неподписанную зону**
  Подписанную версию inline-signing собирает отдельно от исходного файла. Проверяем RRSIG на каждом авторитативном NS, а не только на primary.

- ✕ **Ключи копируют вручную**
  Каталог ключей уезжает rsync без .state-файлов, и named теряет тайминги ротации. Ключи живут в key-directory, бэкап — архивом с правами 600.

- ✕ **Зона подписана, но никто не валидирует**
  Внутренние DNS форвардят на резолвер без валидации — защита не работает. Включаем dnssec-validation на своих серверах и закрываем внешний 53/udp.

- ✕ **Смена алгоритма в лоб**
  Отключение DNSSEC и подписание другим алгоритмом даёт окно BOGUS. Алгоритм меняем правкой policy: BIND сам ведёт двойное подписание и rollover.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Подписать публичные зоны алгоритмом 13 (ECDSAP256SHA256), DS — у регистратора
- NTP на всех авторитативных NS, offset под мониторингом
- Проверка флага ad и наличия DS после каждой правки делегирования
- EDNS0 работает, TCP/53 открыт на периметре в обе стороны

НОРМАЛЬНО

- Перевод зон на dnssec-policy (BIND 9.20) или CSK-режим PowerDNS 5.0
- NSEC3 только с iterations 0 и пустой солью либо чистый NSEC
- Публикация CDS/CDNSKEY и checkds для контроля DS в родителе
- Мониторинг AD-флага и остатка RRSIG с порогом ниже signatures-refresh

ХОРОШО

- Автоматический KSK-rollover: parental-agents плюс rndc dnssec -checkds
- Валидация на внутренних резолверах: RFC 5011, aggressive-nsec, буфер 1232
- Ежеквартальный аудит цепочки доверия по каждой зоне (dnsviz probe и grade)
- Регламент аварийного отката: снятие DS и возврат зоны в insecure

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Все публичные зоны подписаны, и DS опубликован в родительской зоне?
- [ ] Алгоритм подписи — 13 (ECDSAP256SHA256), а не RSA-1024?
- [ ] NSEC3 настроен по RFC 9276: iterations 0, соль пустая?
- [ ] Ключами управляет dnssec-policy, а не ручной dnssec-keygen и cron?
- [ ] Политика прописана явно, а не наследуется от built-in default при апгрейде?
- [ ] Время на всех NS синхронизировано, offset попадает в мониторинг?
- [ ] Есть проба флага ad с двух независимых валидирующих резолверов?
- [ ] Порог алерта по остатку RRSIG ниже signatures-refresh (иначе ложные срабатывания)?
- [ ] Каждый secondary отдаёт RRSIG, а не только primary?
- [ ] Описаны процедуры KSK-rollover и аварийного возврата зоны в insecure?

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 зон и делегирования: цепочка доверия, EDNS0, TTL, готовность к подписанию
- Подписание зон на BIND 9.20 или PowerDNS 5.0 с переводом на dnssec-policy
- Публикация DS у регистратора и настройка CDS/CDNSKEY для автоматики
- Мониторинг AD-флага и остатка подписей в Zabbix с алертом в Telegram
- Регламент KSK/ZSK-rollover и аварийного отката, обучение админов клиента

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 BIND 9 ARM: блок dnssec-policy и встроенная policy default (bind9.readthedocs.io — 9.20)

02 BIND 9 DNSSEC Guide и man rndc: dnssec -status, dnssec -checkds (bind9.readthedocs.io — 9.20)

03 PowerDNS Authoritative: DNSSEC operational, man pdnsutil (zone ...) (doc.powerdns.com — 5.0)

04 Knot DNS Configuration Reference: policy, ksk-submission (knot-dns.cz — 3.4)

05 Unbound unbound.conf: trust anchors, aggressive-nsec, буферы (unbound.docs.nlnetlabs.nl — 1.25)

06 Zabbix: элементы данных агента 2, ключ net.dns.get и его флаги (zabbix.com — 7.0)

07 RFC 9276 (NSEC3), RFC 7344 и 8078 (CDS/CDNSKEY и DS), RFC 5011 (rfc-editor.org — 2007-22)

08 Наш шаблон Zabbix и регламент эксплуатации DNSSEC-зон ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.