



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

12 шагов подготовки медклиники к изоляции рунета

Как мы локализуем DNS, почту, CRM и печать в контуре
клиники и строим 4 уровня резерва канала

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Медклиника на 25 РМ живёт на внешних сервисах: запись пациентов через мессенджер-бота, почта и документы в облаке, CRM в SaaS, отчётность и банк-клиент онлайн. Любой сбой внешней связности останавливает регистратуру, печать этикеток на пробирки и обмен с лабораториями. Мы заранее локализуем критичные сервисы в контуре клиники и строим многоуровневый резерв каналов.

Почему это важно бизнесу

- День простоя регистратуры клиники на 25 РМ — 180–220 тыс. ₽ недополученной выручки и отток записанных пациентов
- Срыв маркировки пробирок и отправки биоматериала — не ИТ-сбой, а прямой риск для лечебного процесса и репутации
- Недоступность CRM и расписания парализует call-центр: администраторы не видят ни записей, ни контактов пациентов
- Лежащий банк-клиент и просрочка отчётности — пени и блокировки, которые дороже всей подготовки



Ключевые параметры реализации

86400 с

serve-expired-ttl в unbound: сутки
отдаём последний известный
ответ, если форвардеры легли

по докам Unbound 1.25

10 с

интервал check-gateway=ping: два
тайм-аута подряд — шлюз
unreachable, уходим на LTE-резерв

по докам MikroTik ROS 7

3 SIM

три miniSIM-слота в MikroTik LtAP:
netwatch-скрипт перебирает
операторов при деградации канала

по докам MikroTik LtAP

8 ГБ

RAM под mailcow на 25 ящиков
(Postfix/Dovecot/Rspamd/SOGo) —
минимум по доке 6 ГиБ + 1 ГиБ
swap

по докам mailcow

3600 с

TTL MX/A-записей держим заранее:
переключение почты на on-prem
укладывается в 4 часа

наш стандарт

36 ч

DR-учение каждые 6 мес:
физически гасим оптику и
работаем только на LTE-резерве

наш регламент DR



Локальный DNS и зеркала пакетов

Что настраиваем

Офисный сервер клиники (Ubuntu 22.04 LTS): *unbound* + *Verdaccio* + *devpi* + *Nexus Repository CE*

Как мы это делаем

- 1 Ставим *unbound*: `serve-expired: yes`, `serve-expired-ttl: 86400`, `prefetch: yes`; форвардеры по DNS-over-TLS, российский резолвер первым в списке
- 2 Раздаём этот сервер как *primary DNS* на все 25 РМ через DHCP (option 006) — GPO-политика «DNS Servers» на клиентах не применяется, полагаться на неё нельзя
- 3 *Verdaccio* 6 в *Docker* (порт 4873) как *uplink*-прокси *npmjs* с кэшем тарболов на диск; в *.npmrc* разработчика — `registry` на локальный адрес
- 4 *devpi-server* под *PyPI* (порт 3141) и *Nexus Repository CE* 3 как проху-репозитории *Maven/Docker/Helm*; прогрев кэша через `npm ci` и `pip install` по `lock`-файлам всех проек...

РЕЗУЛЬТАТ

При падении внешних резолверов офис продолжает резолвить всё, что было в кэше за сутки; разработчик собирает и деплоит бота записи из локальных зеркал. DNS перестаёт быть единой точкой отказа для 90% сервисов клиники.

КЛЮЧЕВОЙ НЮАНС

Кэш «по запросу» пуст, пока не прогреет: после развёртывания гоняем `npm ci` и `pip install` по `lock`-файлам.
`serve-expired-client-timeout` (по умолчанию 1800 мс с версии 1.23) отдаёт клиенту `stale`-ответ, не дожидаяс...



Почта и CRM внутри контура

Что настраиваем

mailcow: dockerized на офисном сервере (8 ГБ RAM, 200 ГБ NVMe) + self-hosted Bitrix24 на BitrixVM

Как мы это делаем

- 1 Разворачиваем mailcow на параллельном домене: Postfix/Dovecot/Rspamd/SOGo, ежедневный backup_and_restore.sh на отдельный диск
- 2 Внутреннюю переписку сразу переводим на on-prem — это ежедневный боевой прогон нагрузки; внешняя почта пока остаётся в облаке
- 3 TTL MX/A снижаем до 3600 заранее; регламент переключения на on-prem — 4 часа, с проверкой SPF/DKIM/DMARC для нового отправителя
- 4 Bitrix24 self-hosted на BitrixVM v9.x: cron-скрипт ежечасно забирает сделки из облака через REST (crm.deal.list, фильтр >DATE_MODIFY, overlap 25 ч) и пишет в контур

РЕЗУЛЬТАТ

Почта и база пациентов переживают недоступность облаков: on-prem копия отстаёт максимум на час, переключение отрепетировано и укладывается в регламент. Внутренние письма вообще не покидают контур клиники.

КЛЮЧЕВОЙ НЮАНС

Обратную синхронизацию (контур→облако) не включаем без маппинга ID — иначе дубли сделок. И заранее проверяем grace-period лицензий self-hosted ПО при недоступности серверов активации вендора.



Резерв канала, печать и DR-учения

Что настраиваем

MikroTik LtAP (RouterOS 7, 3 miniSIM) + print-сервер Windows Server 2022 + регламент DR

Как мы это делаем

- 1 Failover на рекурсивных маршрутах: default через внешние target, check-gateway=ping, distance 1/2/3; шлюз оператора не пингуем — он отвечает и при мёртвом канале
- 2 Netwatch следит за внешней доступностью и шлёт алерт в Telegram-бот мониторинга при каждом уходе на резерв
- 3 Критичные принтеры (этикетировщик пробирок Zebra, Kyocera) — по USB в print-сервер; подключения и драйверы раскатаны через GPO, очередь живёт без интернета
- 4 Каждые 6 мес — DR-учение 36 ч: физически отключаем оптику, работаем на LTE, дефекты фиксируем в протокол и закрываем за 2 недели

РЕЗУЛЬТАТ

Переключение на LTE происходит за секунды и видно мониторингу, а не пациентам в регистратуре. Печать этикеток и документов не зависит от внешней связности. Каждое учение находит 2-3 реальных дефекта, которые в бою стоили бы часов простоя.

КЛЮЧЕВОЙ НЮАНС

На учениях всплывает то, чего нет в конфигах: особенности мобильного трафика операторов, тайм-ауты веб-клиентов на высокой латентности LTE. Поэтому тест только физический — «на бумаге» не считается.



Подводные камни

✗ DNS-кэш без `serve-expired`

По умолчанию unbound выбрасывает просроченные записи — при падении форвардеров офис слепнет. Включаем `serve-expired: yes` и `serve-expired-ttl: 86400`.

✗ Пинг шлюза оператора вместо интернета

Шлюз LTE отвечает даже при мёртвом канале — failover не срабатывает. Строим рекурсивные маршруты с проверкой внешних target через target-score.

✗ Непрогретое зеркало пакетов

Verdaccio/devpi кэшируют только скачанное: в час X нужного пакета нет. После развёртывания прогреваем кэш `npm ci` и `pip install` по lock-файлам.

✗ MX с суточным TTL

При TTL 86400 переключение почты растянется на сутки у части получателей. Заранее держим TTL 3600 и репетируем перенос MX на on-prem.

✗ Синхронизация CRM в обе стороны без маппинга

Обратная запись в облако без таблицы соответствия ID плодит дубли сделок. Синхронизируем в одну сторону с overlap 25 ч по DATE_MODIFY.

✗ Сетевые принтеры за общим роутером

Перезагрузка роутера сбрасывает сетевые принтеры и очереди. Критичный этикетировщик пробирок подключаем по USB напрямую к print-серверу.

✗ Онлайн-активация self-hosted лицензий

Часть ПО периодически сверяет лицензию с серверами вендора и блокируется без связи. Проверяем grace-period до покупки, а не в час X.

✗ Мониторинг молчит про уход на резерв

Канал упал, LTE подхватил — и никто не знает, что резерва больше нет. Netwatch-алерт в Telegram при каждом переключении маршрута.

Как правильно

МИНИМУМ

- Локальный unbound с serve-expired; primary DNS на всех PM через DHCP option 006
- LTE-резерв хотя бы с одной SIM и авто-failover по рекурсивному маршруту
- Риск-карта внешних зависимостей: альтернатива, время и владелец переключения
- TTL MX/A-записей снижен до 3600 заранее

НОРМАЛЬНО

- Mailcow on-prem параллельным доменом, внутренняя почта уже в контуре
- Зеркала npm/PyPI (Verdaccio 6 + devpi) с прогревом по lock-файлам
- 3 miniSIM разных операторов в LtAP + netwatch-алерты о каждом переключении
- Print-сервер с USB-подключением критичных принтеров, раскатка GPO

ХОРОШО

- Self-hosted Bitrix24 с почасовой синхронизацией сделок из облака
- Nexus Repository CE 3: проху-репозитории Maven/Docker/Helm на вырост
- DR-учение 36 ч каждые 6 месяцев с физическим отключением оптики
- Офлайн-карты и резервный домен .рф, дублирующий сайт клиники



Чек-лист самопроверки

- | | |
|--|---|
| ☐ Отдаёт ли офисный DNS ответы из кэша при падении всех форвардеров (serve-expired: yes включён)? | ☐ Печатаются ли этикетки на пробирки и документы при полностью недоступном внешнем канале? |
| ☐ Есть ли риск-карта: по каждому внешнему сервису — альтернатива, время переключения и ответственный? | ☐ Прогреты ли зеркала пакетов по lock-файлам всех проектов, а не «как получится»? |
| ☐ Готова ли почта в контуре: on-prem сервер обкатан, TTL MX снижен, регламент переключения написан? | ☐ Известен ли grace-period лицензий self-hosted ПО при недоступности серверов активации вендора? |
| ☐ Есть ли копия CRM и базы пациентов внутри офиса и когда последний раз сверяли её актуальность? | ☐ Проводилось ли DR-учение с физическим отключением основного канала за последние 6 месяцев? |
| ☐ Переключится ли интернет на LTE автоматически — и узнает ли об этом мониторинг, а не регистратура? | |

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.



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 внешних зависимостей клиники и риск-карта с временем и стоимостью переключения по каждому сервису
- Разворачиваем контур под ключ: unbound, зеркала пакетов, mailcow, self-hosted CRM на вашем офисном сервере
- Строим многоуровневый резерв канала: MikroTik LtAP + LTE на 3 SIM, рекурсивные маршруты, алерты в Telegram
- Проводим DR-учения 36 ч каждые полгода: протокол дефектов, исправления, отчёт руководству

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



Техническая база

- 01** Unbound — Serving Stale Data (serve-expired) (unbound.docs.nlnetlabs.nl — 1.25)
- 02** unbound.conf(5) — параметры кэша и форвардеров (nlnetlabs.nl — 1.25)
- 03** mailcow: dockerized — Prepare Your System (docs.mailcow.email — 2026)
- 04** RouterOS — Failover (WAN Backup) и Netwatch (help.mikrotik.com — ROS 7)
- 05** Verdaccio — Uplinks и кэширование пакетов (verdaccio.org — v6)
- 06** Sonatype Nexus Repository — Community Edition, proxy-репозитории (help.sonatype.com — 3.77+)
- 07** Курс «Виртуальная машина BitrixVM v9.x» (dev.1c-bitrix.ru — 9.x)
- 08** Шаблон ITfresh: регламент DR-учений 36 ч (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

