



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Immich для бизнеса: self-hosted фотоархив вместо Google Фото

Как мы разворачиваем Immich на 2 млн фото: VectorChord, ML-поиск, бэкап и SSO для юрлиц

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

К нам приходит строительная компания: 12 прорабов, ~2 млн фото объектов за 8 лет (акты, скрытые работы, повреждения) в личных Google Photos. Уволился человек — архив ушёл с ним; фото двухлетней давности для суда не найти; дубликаты плодятся; поиск по IMG_2023.jpg бесполезен. Задача — собрать всё в одном контролируемом месте с рабочим смысловым поиском.

Почему это важно бизнесу

- Архив живёт на личных аккаунтах — с увольнением сотрудника компания теряет доказательную базу по объектам
- Фото для защиты в суде должны находиться за секунды, а не искаться полдня вручную по имени файла
- Коммерческие снимки объектов и персданные нельзя держать в чужом облаке вне контроля компании
- Дубликаты у прораба, менеджера и в папке объекта раздувают хранилище и путают учёт

Ключевые параметры реализации

v1.133+

минимальная версия Immich после миграции на VectorChord — ниже не откатываться

[docs.immich.app /install/upgrading](#)

4 сервиса

server, machine-learning, Redis/Valkey, Postgres-VectorChord в docker compose

офици. docker-compose.yml

0.4.3

версия VectorChord в текущем офици. Postgres-образе Immich; диапазон док $\geq 0.3, < 2.0$

офици. Postgres-образ Immich

nllb-clip

докой рекомендованная мультязычная модель под неанглийский поиск, вкл. русский

[docs](#) — Searching (CLIP-модели)

pg_dumpall

штатный автобэкап БД требует superuser; отдельно бэкапим UPLOAD_LOCATION

[docs](#) — Backup and Restore

$\geq 0.7, < 0.9$

требуемый диапазон pgvector, на котором работает VectorChord

[docs](#) — Postgres (standalone)



Перенос 2 млн фото с личных Google Photos на self-hosted

Что настраиваем

Строительная компания, 12 прорабов, ~2 млн фото за 8 лет, архив в личных аккаунтах

Как мы это делаем

- 1 Сбор источников: Google Takeout, кабель с телефонов, старые флешки бухгалтерии — на промежуточный SSD
- 2 Импорт через Immich CLI: `immich upload --album`; заливка ~1.8 ТБ ~14 ч по гигабиту
- 3 Фоновый ML: распознавание лиц + CLIP-эмбединги; CPU ~80%, ~70 ч на мини-ПК N100 (CPU-only)
- 4 Мобильный клиент 12 прорабам, автозагрузка только по Wi-Fi, чтобы не жечь моб. трафик
- 5 Обучение: 2 ч сотрудникам + час бухгалтерии и юристу по выемке фото для суда

РЕЗУЛЬТАТ

Поиск «акт на Тверской, май 2024» — 3 секунды вместо часа ручного перебора. Архив уволенного электрика — по клику на лицо плюс фильтр по дате. Весь фонд в одном контролируемом месте за VPN-периметром.

КЛЮЧЕВОЙ НЮАНС

ML-индексация — самый долгий этап. На CPU-only мини-ПК закладываем 3-5 суток на первичную обработку и не запускаем клиента раньше, чем прогреются лица, CLIP и превью.



Docker-стек и обязанка безопасности под юрлицо

Что настраиваем

Тот же клиент: Debian 12 + Docker, мини-ПК N100, JBOD 4×4 ТБ в ZFS RAID-Z1

Как мы это делаем

- 1 docker compose: immich-server, immich-machine-learning, Redis/Valkey, Postgres на образе 14-vectorchord
- 2 nginx + Let's Encrypt; наружу порт не публикуем — доступ только через WireGuard, мобильный клиент по VPN
- 3 SSO через Authentik (OAuth): логины = рабочая почта; 2FA TOTP обязателен администраторам
- 4 Роли на альбомы: прораб — свои объекты, бухгалтерия — read-only, директор — всё
- 5 Restic каждую ночь в S3 РФ-провайдера, шифрование, ключ хранится только у клиента

РЕЗУЛЬТАТ

Уволенный сотрудник отключается одной кнопкой в SSO, фото остаются в архиве. Корзина 90 дней спасает от «почистил лишнее». Данные полностью в собственности компании, а не в чужом облаке.

КЛЮЧЕВОЙ НЮАНС

Immich из коробки — личный инструмент. Под бизнес докручиваем SSO, VPN-периметр, ролевой доступ и офсайт-бэкап: сам Immich копий наружу не делает, это наша обязанка.



Проверяемый бэкап: дампы БД + UPLOAD_LOCATION

Что настраиваем

Наш регламент для всех Immich-внедрений на абонентском обслуживании

Как мы это делаем

- 1 Ночью: pg_dumpall под superuser → сжатый дампы; отдельно Restic по UPLOAD_LOCATION (library, upload, profile, thumbs)
- 2 Restic в S3 РФ-провайдера: шифрование и ретенция, ключ вне самого сервера
- 3 Раз в квартал — тестовый развёртыш на чистой VM из дампа плюс файлов
- 4 Сверяем версии Immich и VectorChord: после миграции не откатываемся ниже v1.133

РЕЗУЛЬТАТ

Тестовое восстановление ловит рассинхрон версий Postgres-образа и расширения раньше, чем это случится в проде. Клиент видит, что архив реально поднимается, а не «вроде бэкапится».

КЛЮЧЕВОЙ НЮАНС

Дампы БД без папок фото (или наоборот) бесполезен: миниатюры и эмбеддинги привязаны к базе. Бэкапим и БД, и файлы, и всегда проверяем распаковкой на отдельной VM.



Подводные камни

✗ Бэкап только БД без файлов

Дамп Postgres без UPLOAD_LOCATION (library/upload/thumbs) не восстановит архив — превью и эмбеддинги привязаны к базе.

✗ Откат ниже v1.133 после VectorChord

После миграции pgvecto.rs→VectorChord даунгрейд Immich ломает БД; фиксируем нижнюю границу версии в регламенте.

✗ Автообновление раз в неделю вслепую

Immich релизится еженедельно и помечен как активно разрабатываемый: читаем release notes, ждём breaking changes, тестируем.

✗ Immich торчит в интернет

Дефолтный Immich — личный, без корпоративной защиты; прячем за WireGuard и reverse-proxy, порт наружу не публикуем.

✗ Ставка на OCR как на факт

Распознавание текста на фото в ядре Immich не гарантировано; поиск строим на CLIP и лицах, OCR проверяем на данных клиента.

✗ GPU считают обязательным

Первичная ML-индексация тяжёлая, но идёт и на CPU; GPU ускоряет, но не обязателен — закладываем время, а не переплату за карту.

✗ Один диск без RAID

2 млн фото на одиночном HDD — потеря архива при отказе; минимум RAID-Z1 или mirror плюс офсайт-копия.

✗ pg_dumpall без superuser

Штатный автобэкап требует прав суперпользователя Postgres; иначе готовим БД по инструкции docs заранее.



Как правильно

МИНИМУМ

- Один сервер, docker compose из 4 сервисов, диск в RAID-Z1 или mirror
- Nightly-дамп БД + копия UPLOAD_LOCATION на отдельный носитель
- Доступ только по VPN, порт Immich наружу закрыт

НОРМАЛЬНО

- Офсайт-бэкап Restic в S3 с шифрованием, ключ у клиента
- SSO (Authentik/Keycloak), 2FA TOTP админам, роли на альбомы
- Мониторинг SMART и заполненности, алерт в Telegram при 80%
- Обновления по release notes с оглядкой на breaking changes

ХОРОШО

- Ежеквартальный тест восстановления на чистой VM
- Аппаратное ускорение ML (OpenVINO/CUDA) при больших потоках
- Мультиязычная CLIP-модель (nllb/XLM/SigLIP2) под русскоязычный поиск
- Корзина 90 дней и разграничение прав до уровня объектов



Чек-лист самопроверки

- | | |
|---|--|
| ☐ Посчитать объём: число фото, суммарные ТБ, прирост в месяц — под ёмкость диска и время ML-индексации | ☐ Настроить SSO и 2FA TOTP админам, роли на альбомы (read-only бухгалтерии) |
| ☐ Собрать источники: Google Takeout, телефоны, флешки — на промежуточный SSD перед импортом | ☐ Nightly: дампы БД + бэкапы UPLOAD_LOCATION, Restic в S3 с шифрованием |
| ☐ Развернуть docker compose: server, machine-learning, Redis/Valkey, Postgres на образе 14-vectorchord | ☐ Зафиксировать версии Immich и VectorChord, не откатываться ниже v1.133 |
| ☐ Импорт через immich CLI (immich upload --album), контролировать нагрузку CPU при ML | ☐ Раз в квартал разворачивать бэкапы на тестовой VM и сверять целостность |
| ☐ Закрывать Immich за WireGuard и reverse-прокси, порт наружу не публиковать | ☐ Мобильный клиент сотрудникам, автозагрузка только по Wi-Fi |

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).

- Бесплатный аудит по Москве и области: посчитаем объём архива, подберём железо и смету переноса
- Развернём Immich под ключ: docker-стек, ZFS-хранилище, VPN-периметр, SSO и 2FA
- Перенесём фото из Google Photos, с телефонов и флешек, настроим ML-поиск и альбомы
- Настроим зашифрованный офсайт-бэкап в S3 РФ-провайдера с ежеквартальной проверкой восстановления
- Возьмём на абонентку: обновления по release notes, мониторинг дисков, помощь сотрудникам

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** Immich Docs — Upgrading (миграция pgvecto.rs → VectorChord) (docs.immich.app — 2026)
- 02** Immich Docs — Pre-existing / Standalone Postgres (docs.immich.app — 2026)
- 03** Immich Docs — Backup and Restore (pg_dumpall, UPLOAD_LOCATION) (docs.immich.app — 2026)
- 04** Immich Docs — Smart Search и выбор CLIP-модели (docs.immich.app — 2026)
- 05** Immich Docs — Hardware-accelerated Machine Learning (docs.immich.app — 2026)
- 06** Immich — официальный docker-compose.yml (4 сервиса) (github.com/immich-app — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

