Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Bitwarden на своём сервере: разворачиваем за два часа

Наш стандарт: Vaultwarden 1.37.2 или Bitwarden lite, Argon2id, TLS, бэкап и отзыв доступа

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У компаний до 50 рабочих мест пароли к 1С, банк-клиенту, хостингу и рекламным кабинетам живут в чате, в xlsx на общей шаре и в браузерных профилях. Полного списка доступов нет, отзыв при увольнении делается вручную и неполно. Мы закрываем это одним контуром: свой сервер Bitwarden-совместимого хранилища с организацией, коллекциями, ролями, 2FA и журналом событий.

Почему это важно бизнесу

- Отзыв доступа при увольнении — одна операция в организации, а не обход десяти систем вручную
- Полный реестр доступов компании: видно, кто и к какой коллекции допущен, и когда запись менялась
- Пароли к системам с персданными хранятся шифрованно на своём железе — снимаем вопрос 152-ФЗ по хранению
- Нет валютной подписки на пользователя: расходы — только VPS или ВМ на своём гипервизоре
- Отказ сервера не останавливает работу: клиенты держат локально расшифровываемую копию хранилища

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

1.37.2

версия Vaultwarden в нашем стандарте: обязательна для клиентов 2026.8.0 и новее

релиз Vaultwarden 1.37.2, 08.2026

200 МБ RAM

минимум для Bitwarden lite (ghcr.io/bitwarden/lite) плюс 1 ГБ диска и Docker Engine 26+

документация Bitwarden lite, 2026

2 ГБ / 12 ГБ

минимум RAM и диска для Bitwarden Linux Standard; рекомендуем 4 ГБ и 25 ГБ

документация Bitwarden, 2026

600 000

итераций PBKDF2-SHA256: дефолт и минимум с релиза 2026.2.1; в Vaultwarden столько же

документация Bitwarden, 2026

64 MiB / 3

наш профиль Argon2id (parallelism 4) вместо дефолта 32 MiB и 6 итераций

стандарт ITfresh поверх дефолта Bitwarden

20 мин

ADMIN_SESSION_LIFETIME по умолчанию; ADMIN_RATELIMIT_SECONDS=300, burst 3

.env.template Vaultwarden 1.37.2

РЕАЛИЗАЦИЯ 1 ИЗ 3

Юрфирма 8 PM: Vaultwarden на VPS в РФ за два часа

Что настраиваем

1 vCPU / 1 ГБ RAM, Ubuntu 24.04, Docker Engine 26+, контейнер vaultwarden/server:1.37.2 за nginx

Как мы это делаем

1. Разворачиваем docker compose: том /data, DOMAIN=https://vault.<домен>, ENABLE_WEBSOCKET=true, порты контейнера наружу не публикуем — только на 127.0.0.1
2. nginx как reverse proxy: TLS от Let's Encrypt, HSTS, проксирование /notifications/hub с Upgrade и Connection, IP_HEADER=X-Real-IP
3. Закрываем регистрацию: SIGNUPS_ALLOWED=false, INVITATIONS_ALLOWED=true, ORG_CREATION_USERS=none, ADMIN_TOKEN — строка Argon2id PHC от `vaultwarden hash`
4. Создаём организацию, коллекции «Общее / Бухгалтерия / IT / Внешние кабинеты», роли Owner-Admin-User, включаем ORG_EVENTS_ENABLED=true и EVENTS_DAYS_RETAIN=365
5. Импорт из браузеров и xlsx, ротация всех перенесённых паролей, TOTP-2FA на всю организацию, проверка автозаполнения на iOS и Android

РЕЗУЛЬТАТ

Все доступы компании собраны в один реестр за рабочий день. Пароли, которые лежали в общем чате, сменены и разложены по коллекциям с точечным доступом. Расход на инфраструктуру — одна VPS, лицензий на пользователя нет.

КЛЮЧЕВОЙ НЮАНС

Порядок операций важен: сначала SIGNUPS_ALLOWED=false и TLS, только потом первый вход и импорт. Иначе форма регистрации несколько часов открыта всему интернету.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Медклиника 20 PM: Bitwarden lite на своём гипервизоре

Что настраиваем

ВМ 2 vCPU / 2 ГБ, образ ghcr.io/bitwarden/lite + внешний PostgreSQL, публикация только в LAN и через VPN

Как мы это делаем

1. Получаем installation id и key на bitwarden.com/host, задаём BW_DOMAIN, BW_INSTALLATION_ID, BW_INSTALLATION_KEY в файле settings.env
2. BW_DB_PROVIDER=postgresql, БД на отдельном инстансе: BW_DB_SERVER, BW_DB_DATABASE, BW_DB_USERNAME, BW_DB_PASSWORD; порты BW_PORT_HTTP=8080 и BW_PORT_HTTPS=8443
3. Терминация TLS на фронтовом nginx, BW_ENABLE_SSL=false внутри контейнера, наружу за периметр 8080 не выпускаем — доступ только через VPN
4. KDF организации переводим на Argon2id 64 MiB / 3 итерации / parallelism 4, требуем 2FA у всех, включаем журнал событий (BW_ENABLE_EVENTS=true)
5. Бэкап: ночной pg_dump плюс снапшот тома с вложениями на Veeam, ежемесячная проверка восстановлением на тестовой ВМ

РЕЗУЛЬТАТ

Хранилище доступов к МИС, банк-клиенту и кабинетам не покидает контур клиники, а восстановление проверено практикой, а не предположением. Отзыв доступа уволенного сотрудника занимает минуту вместо аудита на день.

КЛЮЧЕВОЙ НЮАНС

Смена KDF перевыпускает ключи у всех и завершает активные сессии: назначаем окно, предупреждаем сотрудников и заранее делаем дамп БД — иначе получаем шквал «не могу войти».

РЕАЛИЗАЦИЯ 3 ИЗ 3

Offboarding и ротация: превращаем хранилище в процесс

Что настраиваем

Регламент по организации целиком: коллекции, роли, 2FA, журнал событий и ежеквартальная ротация

Как мы это делаем

1. Матрица «коллекция → роль → сотрудник» фиксируется письменно, доступ выдаётся только через членство в коллекции, личные шаринги записей запрещены
2. Уволенный: Revoke access участнику в организации, затем принудительная смена всех паролей его коллекций в тот же день
3. Общие технические учётки собираем в отдельную коллекцию и ротируем ежеквартально; TOTP-секреты храним в самой записи, а не в личном телефоне
4. Ежемесячно выгружаем отчёт событий организации и сверяем список участников с кадровым перечнем
5. Обновление контейнера — раз в месяц: docker compose pull, бэкап тома до рестарта, проверка входа с мобильного клиента и синхронизации

РЕЗУЛЬТАТ

Отзыв доступа перестал зависеть от памяти руководителя: revoke в организации плюс ротация паролей коллекций закрывает и корпоративные, и внешние кабинеты за один проход.

КЛЮЧЕВОЙ НЮАНС

Удаление участника не отменяет того, что он уже видел и мог сохранить локально. Реальный отзыв — это revoke плюс смена паролей, к которым у него был доступ.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **SIGNUPS_ALLOWED оставлен в true**
  Дефолт Vaultwarden — открытая регистрация: любой из интернета заведёт аккаунт на вашем сервере. Ставим false и приглашаем через INVITATIONS_ALLOWED.

- ✕ **ADMIN_TOKEN простой строкой**
  Плоский токен утекает в дампах окружения и логах. Генерируем `vaultwarden hash`, строку $argon2id$... в кавычках, в compose $ экранируем как $$.

- ✕ **Админ-панель открыта в интернет**
  Путь /admin закрываем на реверс-прокси по IP или VPN. ADMIN_RATELIMIT_SECONDS=300 и burst 3 — тормоз для перебора, а не замена ограничению доступа.

- ✕ **Бэкап только тома /data**
  При ENABLE_DB_WAL=true копия db.sqlite3 без `sqlite3 .backup` бьётся. Отдельно копируем attachments, sends, config.json и rsa_key.pem.

- ✕ **Пароли перенесли, но не сменили**
  Перенос из чата и xlsx не отменяет компрометации: пароль видели все в переписке. Каждую импортированную запись ротируем сразу после переноса.

- ✕ **2FA только у директора**
  Без обязательной двухфакторной аутентификации мастер-пароль — единственный барьер. Включаем TOTP всем участникам и политику 2FA в организации.

- ✕ **Восстановление ни разу не проверено**
  Бэкап без теста восстановления — не бэкап. Раз в месяц поднимаем копию на тестовой ВМ и проверяем вход и расшифровку записей.

- ✕ **Синхронизация настроена не до конца**
  Без Upgrade-заголовков на /notifications/hub нет живого обновления в вебе и расширении, а мобильным нужен PUSH_ENABLED=true с id и key от Bitwarden.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Docker Engine 26+, отдельный том под данные, DOMAIN строго на https
- TLS Let's Encrypt с автопродлением, HTTP только редирект на HTTPS
- SIGNUPS_ALLOWED=false, ORG_CREATION_USERS=none, регистрация по инвайтам
- Ежедневный дамп базы и тома вложений на внешнее хранилище

НОРМАЛЬНО

- Argon2id 64 MiB / 3 итерации / parallelism 4 вместо PBKDF2
- Обязательная TOTP-2FA всем участникам организации
- Коллекции по отделам, роли Owner/Admin/User, доступ только через коллекцию
- ORG_EVENTS_ENABLED=true, EVENTS_DAYS_RETAIN=365, сверка участников с кадрами

ХОРОШО

- Админ-панель и веб-хранилище доступны только из LAN и через VPN
- SMTP_SECURITY=starttls, SMTP_PORT=587 для инвайтов и оповещений о входе
- Ежемесячное обновление образа с бэкапом до рестарта и проверкой входа
- Ежеквартальная ротация общих техучёток и проверка восстановления из копии

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Регистрация закрыта: SIGNUPS_ALLOWED=false, приглашения включены?
- [ ] ADMIN_TOKEN задан строкой Argon2id PHC, а не открытым текстом?
- [ ] Путь /admin ограничен по IP или доступен только через VPN?
- [ ] На домене валидный TLS с автопродлением и редиректом с 80 порта?
- [ ] KDF организации переведён на Argon2id, а не оставлен на PBKDF2?
- [ ] TOTP-2FA включена у всех участников, включая технические учётки?
- [ ] Есть ежедневный дамп базы, вложений и rsa_key.pem вне этого хоста?
- [ ] Восстановление из бэкапа проверялось на тестовой ВМ за последний месяц?
- [ ] Импортированные из чатов и файлов пароли ротированы после переноса?
- [ ] Есть регламент offboarding: revoke в организации плюс смена паролей коллекций?

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).

- Разворачиваем Vaultwarden или Bitwarden lite на вашей ВМ или VPS за один рабочий день
- Проектируем коллекции и роли под структуру компании, включаем 2FA и журнал событий
- Переносим пароли из браузеров, чатов и xlsx с обязательной ротацией каждой записи
- Настраиваем бэкап базы и вложений с ежемесячной проверкой восстановления
- Ведём регламент отзыва доступа и ротации техучёток в рамках абонентского обслуживания

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 Self-host Bitwarden: Linux Standard Deployment (bitwarden.com/help — 2026)

02 Bitwarden lite Deployment: установка и переменные (bitwarden.com/help — 2026)

03 Encryption Key Derivation: PBKDF2 и Argon2id (bitwarden.com/help — 2026)

04 Vaultwarden: релизы 1.36–1.37.2 и wiki проекта (github.com/dani-garcia — 2026)

05 Vaultwarden .env.template: полный список переменных (github.com/dani-garcia — 1.37.2)

06 Регламент внедрения парольного хранилища ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.