Password Management Features

Новые страницы

1. Страница настроек - `/dashboard/settings`

Страница для смены пароля авторизованного пользователя.

Функционал:
- Форма смены пароля с тремя полями:
- Текущий пароль
- Новый пароль (минимум 8 символов)
- Подтверждение нового пароля
- Валидация на клиенте:
- Проверка минимальной длины пароля
- Проверка совпадения нового пароля и подтверждения
- Проверка, что новый пароль отличается от старого
- Отображение ошибок и успешных сообщений
- Кнопка возврата к дашборду

API эндпоинт: `POST /v2/auth/change-password`

2. Страница восстановления пароля - `/forgot-password`

Страница для запроса восстановления пароля.

Функционал:
- Форма с полем email
- Отправка запроса на восстановление пароля
- Отображение успешного сообщения после отправки
- Ссылка для возврата к странице входа

API эндпоинт: `POST /v2/auth/forgot-password`

Примечание: В MVP версии токен выводится в консоль бэкенда. В production нужно настроить email сервис.

3. Страница сброса пароля - `/reset-password`

Страница для установки нового пароля по токену из email.

Функционал:
- Получение токена из URL параметра `?token=...`
- Форма с двумя полями:
- Новый пароль (минимум 8 символов)
- Подтверждение пароля
- Валидация на клиенте
- Отображение ошибок (невалидный/истекший токен)
- Успешное сообщение с кнопкой перехода к входу

API эндпоинт: `POST /v2/auth/reset-password`

Изменения в существующих страницах

Страница входа - `/login`

Добавлено:
- Ссылка “Забыли пароль?” под формой входа
- Обновлен эндпоинт с `/v2/auth/token` на `/v2/auth/login`
- Изменен формат запроса с `application/x-www-form-urlencoded` на `application/json`

Дашборд - `/dashboard`

Добавлено:
- Ссылка “Настройки” в боковом меню навигации

Интеграция с бэкендом

Все запросы используют:
- `credentials: 'include'` для отправки httpOnly cookies
- Функции `fetchJSON` и `fetchAuthJSON` из `lib/api.ts`
- Автоматическая обработка ошибок 401 (перенаправление на `/login`)

Безопасность

- Все формы используют `type="password"` для полей паролей
- Минимальная длина пароля: 8 символов
- Валидация на клиенте перед отправкой на сервер
- httpOnly cookies для защиты токенов
- Токены сброса пароля действительны 1 час

Дизайн

Все новые страницы используют единый стиль:
- Градиентный фон (purple-50 → white → blue-50)
- Белые карточки с тенью
- Фиолетово-синие градиентные кнопки
- Адаптивный дизайн
- Иконки для визуальной обратной связи

Тестирование

Локальный запуск

```
npm run dev
```

Тестовый сценарий

1. Зарегистрировать пользователя через `/v2/auth/register`
2. Войти через `/login`
3. Перейти в `/dashboard/settings` и сменить пароль
4. Выйти и попробовать войти со старым паролем (должна быть ошибка)

5. Войти с новым паролем
6. Перейти на `/forgot-password` и запросить восстановление
7. Скопировать токен из консоли бэкенда
8. Перейти на `/reset-password?token=<токен>`
9. Установить новый пароль
10. Войти с новым паролем

Переменные окружения

Убедитесь, что в `.env.local` указан правильный URL бэкенда:

```
NEXT_PUBLIC_API=http://localhost:8000
```

Для production:

```
NEXT_PUBLIC_API=https://api.upak.space
```

Следующие шаги

После мерджа:
1. Настроить email сервис на бэкенде для отправки токенов
2. Добавить rate limiting для защиты от брутфорса
3. Добавить капчу на формы восстановления пароля
4. Добавить историю смены паролей
5. Добавить двухфакторную аутентификацию (опционально)