Урок 12. Двухфакторная аутентификация (2FA) в Work List Planner

Дата: 19 октября 2026 года
Проект: Work List Planner
Тема: Усиление безопасности авторизации и подключение двухфакторной защиты.

1. Цель занятия

Реализовать полноценную двухфакторную аутентификацию, чтобы одного пароля было недостаточно для входа в аккаунт при включённой защите.

В качестве второго фактора используется одноразовый шестизначный код из приложения-аутентификатора. Дополнительно предусмотрены резервные коды на случай потери доступа к приложению.

2. Что реализовано

2.1. Серверная часть

В backend на FastAPI реализованы механизмы:

- Генерация секрета TOTP для пользователя.
- Шифрование секрета перед сохранением в базе данных.
- Проверка одноразовых кодов.
- Подтверждение подключения 2FA.
- Генерация резервных кодов и хранение их хешей.
- Проверка второго фактора при входе в систему.
- Инвалидация прежней версии токена после включения защиты.

Основные маршруты API:

Маршрут	Назначение
`POST /users/me/2fa/setup`	Подготовка подключения 2FA и получение QR-кода
`POST /users/me/2fa/confirm`	Подтверждение подключения шестизначным кодом
`POST /token`	Авторизация с проверкой второго фактора, если он включён

При включённой 2FA пользователь должен предоставить пароль и TOTP-код либо резервный код.

2.2. Клиентская часть

В `index.html` добавлена панель управления двухфакторной защитой.

Пользователь может:

1. Открыть панель настройки 2FA.
2. Ввести текущий пароль.
3. Получить QR-код и секретный ключ.
4. Подключить совместимое приложение-аутентификатор.
5. Подтвердить подключение шестизначным кодом.
6. Получить и сохранить резервные коды.

Также была добавлена обработка дополнительного кода при входе в систему в страницах авторизации приложения, включая `index.html`, `budget.html`, `savings.html`, `budget.preview.html` и `admin.html`.

3. Как работает подключение

1. Пользователь открывает панель двухфакторной защиты.
2. Сервер проверяет текущий пароль и создаёт секрет TOTP.
3. Секрет передаётся интерфейсу для настройки приложения-аутентификатора.
4. Пользователь вводит код из приложения.
5. Сервер проверяет код и активирует 2FA.
6. Генерируются резервные коды, предназначенные для восстановления доступа.
7. При последующих входах сервер требует второй фактор.

После активации защиты необходимо выполнить повторный вход, поскольку версия ранее выданного токена становится недействительной.

4. Проверки и результат

В ходе работы выполнены проверки:

- Три теста, относящиеся к 2FA, завершились успешно: `3 passed, 51 deselected, 4 warnings`.
- Локальная HTTP-проверка главной страницы вернула `HTTP 200`.
- Сервис `planner.service` находился в состоянии `active`.
- Панель настройки 2FA добавлена в интерфейс.
- Подключение защиты и последующий вход были проверены вручную.
- Вход с дополнительным фактором работает.

Итог: двухфакторная аутентификация реализована и проверена в рабочем приложении.

5. Важные замечания по безопасности

- Резервные коды необходимо хранить в надёжном месте и не передавать другим людям.
- Секрет TOTP нельзя публиковать или отправлять посторонним.
- Нельзя считать включение 2FA завершённым без проверки повторного входа.
- Перед дальнейшими изменениями авторизации важно сохранять резервные копии изменяемых файлов.
- При последующих доработках необходимо сохранять совместимость между серверной проверкой и всеми формами входа.

6. Итоги занятия

Сегодня мы усилили безопасность Work List Planner и прошли путь от серверной логики до пользовательского интерфейса.

Реализованы:

- серверные механизмы настройки и подтверждения 2FA;
- проверка второго фактора при авторизации;
- резервные коды восстановления;
- интерфейс подключения защиты;
- обработка дополнительного кода на страницах входа.

Главный результат — функция не только реализована, но и проверена в реальном интерфейсе.

7. План следующего занятия

Продолжить развитие Work List Planner с учётом текущего состояния проекта.

При необходимости отдельно проверить сценарии восстановления доступа и отказа второго фактора, затем перейти к следующей задаче проекта. Не повторять уже успешно завершённые проверки без конкретной причины.

Статус урока: завершён.
Статус 2FA: работает.
Дата завершения: 19.10.2026.

Revision #2
Created 2026-10-19 20:16:44 UTC by im
Updated 2026-10-19 20:19:32 UTC by im