ВШЭ Разработка Безопасного ПО

Студент	Крамаренко Михаил
Группа	234

Содержание

1. NFR ≥ 8 с критериями

Файл: NFR.md

Результат: 8 нефункциональных требований безопасности (`NFR-01 – NFR-08`)

Каждое требование содержит:

- формализованное описание цели безопасности,
- метрику/порог проверки,
- способ тестирования (unit/functional tests, code inspection),
- компонент покрытия и приоритет.

Покрытые категории:

- 🔐 Контроль доступа (RBAC)
- 🔑 Безопасное хранение паролей (bcrypt)
- 🚫 Ограничение логина и защиты от brute force
- 🧮 Валидация данных через Pydantic
- ⚙️ Безопасная конфигурация (переменные окружения)
- 🧾 Логирование событий безопасности
- 🛡️ Защита от XSS

- 📦 Ограничение размера запросов

Матрица трассировки: **NFR_TRACEABILITY.md**

- каждая NFR привязана к пользовательским историям или задачам (`US` / `DEV` / `OPS` / `QA`) и релизу `v1.0` .

BDD-приёмка: **NFR_BDD.md**

- сценарии в формате Gherkin для подтверждения выполнения NFR через тесты.

2. 3–4 DFD с границами доверия

Файл: **DFD.md**

Результат: представлена детальная DFD (Data Flow Diagram) уровня контекста и процессов.

Основные особенности:

- Используется Mermaid-диаграмма с выделением двух trust boundaries:
  - 🔴 Edge Boundary — граница между пользователем и системой (внешние взаимодействия);
  - 🟢 Core Boundary — граница между бизнес-логикой и внутренним хранилищем.
- Описано 10 потоков данных (`F1-F10`), включая каналы, тип данных и комментарии.
- Указаны все компоненты системы: User, FastAPI App, Controller, Service, хранилища.

Вывод:
DFD корректно отражает границы доверия, потоки данных и взаимодействия компонентов.

3. STRIDE ≥ 8 угроз

Файл: **STRIDE.md**

Результат: 11 угроз, классифицированных по STRIDE (S/T/R/I/D/E).

Категория	Кол-во угроз	Пример
Spoofing	1	`F1-S` : подделка клиента
Tampering	4	`F1-T` , `F3-T` , `F4-T` , `F5-T`
Repudiation	1	F1-R: отказ от операций
Information Disclosure	3	`F1-I` , `F4-I` , `F5-I`

Категория	Кол-во угроз	Пример
Denial of Service	2	`F1-D`, `F4-D`
Elevation of Privilege	1	`F1-E`

Контроли и ссылки:
Каждая угроза сопоставлена с соответствующим NFR (через колонку “Ссылка на NFR”) и артефактом проверки (тест, лог, HTTPS и др.).

Приоритизация:

- Высокие: `F1-S`, `F1-T`, `F1-I`
- Средние: `F1-D`, `F4-I`, `F3-T`
- Низкие: `F1-R`, `F1-E`, `F4-T` / `F5-T`, `F4-D`, `F5-I`

Обоснование угроз и связь с trust boundaries указаны в отдельном разделе.

4. Меры с трассировкой к угрозам/историям

Файл: **RISKS.md**

Результат: Реестр из 12 рисков с полным трассированием.

Поле	Реализовано
RiskID / Описание	✅
Связь с потоками (F) и NFR	✅
Оценка вероятности и влияния (L, I, Risk=L×I)	✅
Стратегия (снизить/принять и т.п.)	✅
Владелец, срок, критерий закрытия	✅

Примеры трассировки:

- `R1` (Несанкционированный доступ) → `F1-S` + `NFR-01`
- `R2` (Модификация данных) → `F1-T` + `NFR-02`
- `R3` (Утечка данных) → `F1-I` + `NFR-04`
- `R4` (DDoS) → `F1-D` + `NFR-05`

Связь с историями:
через матрицу **NFR_TRACEABILITY.md**
обеспечена сквозная трассировка
`Story → NFR → Threat → Risk → Control`.

5. Приоритизация и оформление

Приоритизация:

- NFR приоритизированы (`High` / `Medium` / `Low`).
- Угрозы STRIDE — по уровням критичности.
- Риски — количественная оценка по шкале L×I.
- Ключевые риски (≥15) выделены как критические с датами устранения.

Оформление:

- Все документы выдержаны в едином стиле Markdown.
- Таблицы стандартизированы, поля заполнены.
- Визуализация DFD в Mermaid.
- BDD сценарии читаемы и проверяемы.
- Трассировка и связи представлены во всех документах.

Итоговая оценка по чек-листу (5×2 балла)

Критерий	Балл	Обоснование
NFR ≥ 8 с критериями	✅ 2/2	8 NFR + метрики + проверки
3–4 DFD с границами доверия	✅ 2/2	2 trust boundaries, 10 потоков
STRIDE ≥ 8 угроз	✅ 2/2	11 угроз + контроли
Меры с трассировкой к угрозам/историям	✅ 2/2	Полная цепочка `Story → NFR → Threat → Risk`
Приоритизация и оформление	✅ 2/2	Единый формат, приоритеты, визуализация