**Функциональные требования:**

1. Регистрация и аутентификация:

- Предоставление возможности регистрации новых пользователей.

- Аутентификация существующих пользователей с использованием безопасного механизма входа.

2. Хранение паролей:

- Возможность добавления, редактирования и удаления паролей от учетных записей.

- Шифрование и безопасное хранение паролей пользователей.

4. Категоризация паролей:

- Возможность организации паролей по различным категориям (например, работа, личное, финансы).

**Не функциональные требования:**

1. Безопасность:

- Приложение должно обеспечивать высокий уровень безопасности для хранения паролей и доступа к ним.

- Соответствие стандартам безопасности, таким как GDPR, HIPAA, или другим отраслевым стандартам безопасности.

2. Производительность:

- Быстрый доступ к хранимым данным паролей, минимальное время ожидания при запросах.

- Эффективное использование ресурсов устройства для минимизации влияния на производительность устройства пользователя.

3. Совместимость:

- Совместимость с основными операционными системами (Windows).

- Интеграция с известными веб-браузерами (Chrome) для автоматического заполнения данных.

4. Удобство использования:

- Интуитивно понятный интерфейс пользователя для людей всех возрастов и уровней технической грамотности.

- Адаптивный дизайн для удобства использования на разных устройствах (компьютеры, смартфоны, планшеты).