Техническое задание на разработку программного обеспечения

«Password Keeper»

Новосибирск

2024

ОГЛАВЛЕНИЕ

[1. Наименование программного продукта 3](#_Toc185282246)

[2. Краткая характеристика области применения 3](#_Toc185282247)

[3. Основания для разработки 3](#_Toc185282248)

[3.1 Основания для проведения разработки 3](#_Toc185282249)

[3.2 Наименование и условное обозначение разработки 3](#_Toc185282250)

[3.3 Цель разработки 3](#_Toc185282251)

[4. Назначение разработки 3](#_Toc185282252)

[4.1 Функциональное назначение 3](#_Toc185282253)

[4.2 Эксплуатационное назначение 3](#_Toc185282254)

[5. Требования к функциональным характеристикам 4](#_Toc185282255)

[6. Состав выполняемых функций 4](#_Toc185282256)

[7. Целевая аудитория 4](#_Toc185282257)

[8. Дизайн 5](#_Toc185282258)

[9. Этапы разработки 6](#_Toc185282259)

[10. Функциональные требования 6](#_Toc185282260)

[11. Технические требования 7](#_Toc185282261)

[12. Требования к контенту 8](#_Toc185282262)

[13. Критерии приемки 8](#_Toc185282263)

# 1. Наименование программного продукта

«Password Keeper»

# 2. Краткая характеристика области применения

«Password Keeper» — это бесплатная база данных паролей, предназначенная для безопасного хранения и управления паролями пользователей.

# 3. Основания для разработки

# 3.1 Основания для проведения разработки

Необходимость выполнить задание с определёнными требованиями для зачёта по дисциплине.

# 3.2 Наименование и условное обозначение разработки

База данных хранения паролей «Password Keeper»

# 3.3 Цель разработки

Основная цель разработки «Password Keeper» заключается в создании надежного, безопасного и удобного инструмента для управления паролями.

# **4. Назначение разработки**

# 4.1 Функциональное назначение

* Хранение паролей: «Password Keeper» позволяет организовывать и хранить пароли в защищенном формате;
* Шифрование: все данные шифруются, обеспечивая безопасность информации от несанкционированного доступа;
* Генерация паролей: программа имеет встроенные возможности для создания сложных и уникальных паролей, что помогает повысить безопасность учетных записей.

# 4.2 Эксплуатационное назначение

* Удобство использования:Благодаря интуитивно понятному интерфейсу, пользователи могут легко находить и управлять своими учетными данными;
* Безопасность: обеспечивает средний уровень защиты данных, что подходит для простых пользователей;
* Доступность: программа доступна на операционных системах Windows, позволяя пользователям иметь доступ к своим паролям в любое время;
* Обновление данных: позволяет легко обновлять пароли, что способствует соблюдению принципов безопасности и регулярной смене паролей;

# 5. Требования к функциональным характеристикам

Программа должна обеспечивать возможность выполнения

перечисленных ниже функций:

1. Общие требования

* Интуитивно понятный интерфейс: Платформа должна обеспечивать простой и понятный интерфейс, который позволяет пользователям легко управлять своими паролями.
* Платформа: Настольное приложение должно быть доступно на операционных системах Windows

1. Регистрация

* Возможность регистрации через логин и пароль.
* Пользователь должен иметь возможность входить в систему с использованием зарегистрированных данных.

1. Хранение паролей

* Позволяет сохранять и шифровать пароли
* Будет встроенный инструмент для создания сложных и безопасных паролей

1. Пользовательское заполнение данных в приложении

* Пользователю необходимо самостоятельно вносить логин, пароль, электронный адрес

# 6. Состав выполняемых функций

* Хранение паролей - безопасное хранение учетных данных в зашифрованной базе данных.
* Генератор паролей - создание сложных паролей для повышения безопасности.

# 7. Целевая аудитория

Основная целевая аудитория:

* Возраст: 16-50 лет.
* Пол: мужчины и женщины.
* Социально-экономический статус: разнообразный, часто профессионалы и фрилансеры с стабильным доходом
* Уровень дохода: ниже среднего, средний и выше среднего.
* Интересы: безопасность данных, защита личной информации
* Ценности: надёжность, отсутствие платных функций
* Использование технологий: активные пользователи компьютера и мобильных устройств, часто работающие с интернет-сервисами
* Примеры пользователей:

1. Фрилансеры и удаленные сотрудники: «Password Keeper» помогает им безопасно хранить пароли для различных платформ и клиентов, что облегчает управление множеством учетных записей.
2. Студенты: могут использовать «Password Keeper» для хранения паролей к образовательным платформам и личным сервисам, а также для защиты информации от несанкционированного доступа.
3. Малый бизнес: владельцы и сотрудники могут использовать «Password Keeper» для совместного использования паролей и управления доступом к важным учетным записям, сохраняя при этом безопасность данных.
4. Геймеры: игроки могут организовать пароли к своим игровым аккаунтам и платформам, минимизируя риск утечки данных.
5. Домашние пользователи: «Password Keeper» помогает защитить личные данные и сохранить пароли для социальных сетей, интернет-банков и других сервисов.

# 8. Дизайн

Общая концепция дизайна

1. Цветовая палитра:

Основной цвет: золотой — используется для заднего фона.

Вторичный цвет: серый — используется для фона главного окна регистрации и кнопок.

Дополнительный цвет: белый — используется для полей ввода, ячеек в боковой панели и таблицы.

Цвета должны быть согласованы с психологией восприятия и вызывать положительные эмоции у пользователей.

1. Шрифт:

* Основной шрифт: Arial

# 9. Этапы разработки

1. Прототипирование;
2. Создание дизайна;
3. Разработка и тестирование;
4. Обучение пользователей.

# 10. Функциональные требования

1. Добавление ячеек и их удаление

1.1. Добавление ячеек

* Пользователь должен нажать на пустом пространстве «+»
* Система должна вывести для ввода поля, где пользователь может указать информацию о сервисе, для которого пользователь сохраняет или генерирует пароль
* **С**истема должна позволять пользователям создавать, изменять и удалять пароли

2. Пользовательский интерфейс

2.1. Регистрация и авторизация

* Пользователь должен иметь возможность зарегистрироваться в приложении с использованием email и пароля.
* Система должна обеспечивать функционал авторизации с возможностью восстановления пароля.
  1. Авторизация и аутентификация
* Система должна проверять учетные данные пользователей при входе и предоставлять доступ только авторизованным пользователям. Это обеспечивает безопасность и конфиденциальность данных пользователей.

3. Административные функции

3.1. Управление пользователями

* Администраторы системы должны иметь возможность управлять учётными записями пользователей, включая создание, изменение и удаление учётных записей.

# 11. Технические требования

1. Архитектура приложения

1.1. Клиентская часть

Использование библиотеки PyQt5 для создания интерфейса.

1.2. Серверная часть

Использование языка программирования Python для обработки запросов.

База данных (PostgreSQL) для хранения информации об учетных данных пользователей.

2. Производительность

2.1. Скорость загрузки

Время загрузки страниц внутри приложения не должно превышать 4 секунд при стандартной нагрузке.

2.2. Нагрузка

Приложение должно выдерживать не менее 1000 одновременных пользователей без снижения производительности.

3. Безопасность

3.1. Защита данных

Все данные пользователей должны храниться в зашифрованном виде.

3.2. Защита от атак

Приложение должно быть защищено от SQL-инъекций, несанкционированного удаленного доступа и других распространенных уязвимостей.

4. Интеграция

4.1 Цель интеграции

Хранение паролей в базе данных PostgreSQL для удобства управления и доступа к ним.

5. Документация

5.1. Пользовательская документация

Подготовка руководства пользователя с описанием функционала приложения.

5.2. Техническая документация

Описание архитектуры приложения, используемых технологий и требований.

# 12. Требования к контенту

1. Грамотность и стиль

1.1. Грамотность: все материалы должны быть написаны без орфографических и грамматических ошибок.

1.2. Стиль написания: текст должен быть простым, понятным и доступным для целевой аудитории, с использованием ясных формулировок.

2. Форматы контента

1.1. Текстовые материалы: основной контент должен включать текст.

1.2. Визуальный контент: изображения внутри программы должны быть высокого качества.

# 13. Критерии приемки

1. Функциональные требования

* Управление паролями
* Создание, редактирование и удаление записей.
* Безопасность
* Шифрование базы данных для защиты информации.

1. Пользовательский интерфейс

* Интуитивно понятный интерфейс для легкости использования.
* Поддержка одного языка**.**

1. Производительность

* Скорость загрузки:
* Время загрузки страниц приложения не должно превышать 3 секунд при стандартных условиях использования.

1. Нагрузка:

Приложение должно выдерживать нагрузку не менее 1000 одновременных пользователей без снижения производительности.

1. Тестирование

* Функциональное тестирование: все функции приложения должны быть протестированы на соответствие требованиям.
* Тестирование на различных версиях операционной системы Windows: приложение должно корректно работать на версиях 7, 10, 11.