ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ Г. МОСКВЫ

«КОЛЛЕДЖ ПРЕДПРИНИМАТЕЛЬСТВА №11»

ЦЕНТР ИНФОРМАЦИОННО–КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

**КУРСОВАЯ РАБОТА**

**Внедрение информационной системы для автоматизации процесса шифрования данных**

по дисциплине /междисциплинарному курсу

**МДК.03.02 Внедрение информационных систем**

специальности: 09.02.07 **Информационные системы и программирование**

|  |  |
| --- | --- |
| Выполнил:  студент ИСиП-25  Кунгурцев Виталий Александрович    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись | Научный руководитель:  преподаватель Центра ИКТ  Диянов Владислав Васильевич  \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  оценка подпись |

Москва, 2021 г.

Содержание

[Введение 3](#_Toc100034695)

[Глава 1. Проектирование менеджера паролей 6](#_Toc100034696)

[1.1 Анализ предметной области 6](#_Toc100034697)

[1.2 Описание требований к практической разработке 7](#_Toc100034698)

[1.3 Рассмотрение существующих аналогов приложения 8](#_Toc100034699)

[1.4 Составление проекта разрабатываемого продукта 11](#_Toc100034700)

[1.4.1 Описание функциональных процессов 11](#_Toc100034701)

[1.4.2 Проектирование базы данных 13](#_Toc100034702)

[1.4.3 Макет и графический дизайн менеджера паролей 16](#_Toc100034703)

[1.5 Выбор инструментов и необходимых средств для реализации проектного решения 21](#_Toc100034704)

[Глава 2. Реализация менеджера паролей 24](#_Toc100034705)

[2.1 Разработка составных элементов 24](#_Toc100034706)

[2.1.1 Разработка базы данных 24](#_Toc100034707)

[2.1.2 Разработка приложения 26](#_Toc100034708)

[2.2 Монтаж установка и настройка 29](#_Toc100034709)

[2.3 Тестирование, ввод в эксплуатацию 29](#_Toc100034710)

[2.4 Разработка сопроводительной документации 30](#_Toc100034711)

[Заключение 30](#_Toc100034712)

[Список используемых источников 32](#_Toc100034713)

[Приложение **Ошибка! Закладка не определена.**](#_Toc100034714)

Введение

Хотя технологии обещают облегчить нашу жизнь, и, как правило, так оно и есть, каждый новый веб-сайт и приложение, на которые мы подписываемся, - это еще один пароль, который мы должны запомнить. Для большинства из них стало невозможным запомнить их все. При создании новой учетной записи веб-сайты требуют, чтобы мы создавали длинные и надежные пароли. В противном случае нам даже не разрешат создать учетную запись. Предполагая, что вы пройдете этап создания учетной записи, вы быстро забудете шифр, который вы только что создали, и смиритесь с использованием “Забыли пароль?” ссылка в качестве опции для ежедневного входа в систему.

Проблема, решаемая в проекте, заключается в низком уровне безопасности пользователей интернета по причине сложности менеджмента большого количества длинных и соответствующих нормам компьютерной безопасности паролей, в связи чего одинаковые или слабые пароли использованы в ряде сервисов. Выход есть - программное приложение, предназначенное для хранения учетных данных в интернете и управления ими, которое также генерирует надёжные. Обычно эти ключи безопасности хранятся в зашифрованной базе данных и блокируются с помощью мастер-пароля. Шифрование использует кибербезопасность для защиты от угадывания ключей безопасности взломщиком и кибератак, включая вредоносные программы и программы-вымогатели. Шифрование данных работает путем защиты передаваемых цифровых данных в облаке и компьютерных системах.

Существующие аналоги имеют гигантские базы пользователей с шифрованными данными, и, к сожалению, они не видят большую выгоду в обновлении уровней безопасности хранения данных. Чтобы поменять старые стандарты, которые были выбраны на этапе создания сервиса, придётся расшифровать абсолютно все пароли и логины, провести хэширование всех паролей заново, что займёт огромное количество времени и средств. Поэтому создание новой информационной системы гарантирует самый высший и современный способ защиты данных пользователей.

Цель: продвинуть безопасность пользователя интернета путем создания автоматизированной системы шифрования, генерации и хранении ключей безопасности на различных платформах.

**Задачи:**

1. Анализировать предметную область;
2. Составить план и требования к разработке информационной системы;
3. Определить особенности информационной системы.
4. Сравнить программы-аналоги и выделить их достоинства и недостатки.
5. Описать функциональные блоки: предназначение, рабочие роли;
6. Составить диаграммы по процессам системы;
7. Составить диаграммы UseCase, последовательности, активности, архитектуры;
8. Составить диаграммы архитектуры;
9. Создать дизайн приложения в графическом редакторе;
10. Определить, для какой платформы будет создана информационная система;
11. Выбрать языки программирования и библиотеки;
12. Построить базу данных;
13. Написать программный код, отвечающий за выполнение процессов;
14. Написать графический интерфейс для приложения;
15. Подключить приложение к БД и реализовать шифровку и расшифровку данных;
16. Протестировать работоспособность приложения и исправить найденные ошибки;
17. Внедрить информационную базу;
18. Разработать сопроводительную документацию.

**Объект исследования:** компьютерная безопасность;

**Предмет исследования:** способы генерации и безопасного хранения данных в базе данных;

**Результат, который будет представлен к защите курсовой работы:** приложение с интуитивным графическим интерфейсом, через которое можно управлять данными пользователя, хранящиеся в зашифрованной базе данных.

Глава 1. Проектирование менеджера паролей

1.1 Анализ предметной области

**Кибербезопасность** — это практика защиты систем, сетей и программ от цифровых атак – кибератак.

**Атака на информационную систему** — это совокупность преднамеренных действий злоумышленника, направленных на нарушение одного из трех свойств информации — доступности, целостности или конфиденциальности. Последствия для жертв могут включать потерю ценных данных, таких как презентации, электронные письма и музыка. У жертв также могут быть украдены данные их банковского счета, деньги или даже их личность. Кроме того, неавторизованные пользователи могут использовать чужой компьютер для нарушения закона, что может привести к возникновению юридических проблем у жертвы.

Один из наиболее распространенных способов проникновения хакеров в компьютеры — **подбор паролей.** Простые и часто используемые пароли позволяют злоумышленникам легко получить доступ к вычислительному устройству и управлять им. Пароль, который трудно угадать, делает процесс очень сложным для хакеров и вынуждает их искать другую цель.

Это является истоком проблемы, с которой люди часто сталкиваются при создании сложных паролей, — боязнь их забыть. Оно не удивительно, если посмотреть на **требования к надёжному паролю в 2022 году:**

* + - 1. Иметь минимальную длину в 12 символов (не менее 12 символов);
      2. Не содержать ваше имя, адрес электронной почты, знаменательные даты, номера телефонов или другую информацию, связанную с вами или вашей компанией;
      3. Быть оригинальным (т.е. не подвергаться ранее раскрытию при утечке данных и не использоваться где-либо еще);
      4. Сочетание строчных и прописных букв, цифр и символов, однако сложность пароля не должна использоваться как фактор при определении надежности пароля.

Большинство пользователей обходят их стороной из-за сложности, особенно учитывая, что абсолютно каждый пароль должен соответствовать этим требованиям. Поэтому существуют особый инструмент для управления большим количеством ключей безопасности под названием «Менеджер паролей».

**Менеджеры паролей** — это приложения, которые генерируют новые случайные пароли для всех сервисов, которые вы хотите сохранить. Они хранят эти учетные данные в безопасном виртуальном хранилище с помощью архитектуры с нулевым разглашением, которая, шифрует пароли до того, как они покинут ваше устройство. Когда они на сервере, даже администратор не может их расшифровать. Единственный пароль, который вам нужно запомнить в менеджере паролей, — это мастер-пароль. Пока он надежный, никто не сможет получить к нему доступ.

**Вывод:** интернет предлагает множество инструментов и возможностей для автоматизации нашей жизни, но на ряду с этим приходит опасность от людей, пытающихся получить к ней доступ. Регулярный доступ к сервисам защищён тайным кодом, называющимся паролем, который предотвращает нежеланный доступ к личной информации.

Проблема, заключается в низком уровне безопасности пользователей интернета по причине сложности менеджмента большого количества длинных и соответствующих нормам компьютерной безопасности паролей, решение которой является использование автоматизированной информационной системы по управлению паролей, берущая на себя все задачи.

1.2 Описание требований к практической разработке

У менеджера паролей одна главная, но очень важная задача – сохранить данные пользователя в безопасности. Для этого были созданы и применяются различные способы, от простых и известных с давних времён (пароль), до современных и только становящихся стандартным инструментом защиты информации, таких как двух факторная аутентификация и биометрические данные, т. е. лицо или отпечаток владельца.

Пользователи интернета выбирают лучшие менеджеры паролей на рынке, которые имеют все эти функции, потому что хотят наивысший уровень защиты, однако приобретая множество преимуществ, из всего этого вытекает один важный недостаток.

Лучшие менеджеры паролей привлекают интерес и доверие пользователей, а они, в свою очередь, привлекают хакеров. Чем популярнее сервис, тем больше атак ему приходится выстаивать, делая его мишенью номер один, ведь если они получат доступ к аккаунту в менеджере, они получат доступ к всем остальным паролям, что хранятся в базе данных.

Создать информационную систему по шифрованию паролей, которую пользователь сможет сам контролировать, не является главной мишенью для хакера, имеет меньшую пользовательскую базу, что позволяет вносить улучшения быстрее и проще, выгодно в плане безопасности и уровня удобства финального результата. Для достижения этой цели необходимо описать

требования для разработки информационной системы.

Автоматизированная информационная система шифрования данных должна:

* Использовать современные стандарты шифрования, которые будут надёжны и в ближайшее будущее;
* Использовать современные стандарты хэширования, которые будут надёжны и в ближайшее будущее;
* Предоставлять полный контроль над своими данными;
* Иметь интуитивный и современный пользовательский интерфейс;
* Использовать методы защиты от известных атак на взлом пароля;

1.3 Рассмотрение существующих аналогов приложения

На текущий момент существует широкий выбор менеджеров паролей, и у каждого есть функционал, которого нет у другого приложения-аналога, но в основном, лучшие менеджеры предоставляют довольно похожий опыт, что делает выбор одного единственного намного сложнее. Для создания наилучшей системы с нуля, нужно сравнить существующие программы аналоги и выявить сильные стороны, за которые они заняли позицию на рынке.

**Zoho Vault**

Предлагает надежный бесплатный план для частных лиц с простым в использовании неограниченным хранилищем паролей и гибкими бизнес-планами для команд.

**Dashlane**

Dashlane упрощает интеллектуальное управление паролями и включает в себя некоторые элементы, ориентированные на безопасность. Однако, чтобы получить все его функции, вам придется много заплатить.

**Bitwarden**

Бесплатный уровень Bitwarden с открытым исходным кодом справляется со всеми ожидаемыми задачами менеджера паролей с удивительно небольшими ограничениями. Его платный уровень добавляет инструменты безопасности и хранения по чрезвычайно низкой цене для этой категории.

**LogMeOnce Password Management Suite Ultimate**

Метод входа по умолчанию не требует пароля и использует аутентификацию на основе смартфона. Этот превосходный продукт имеет больше функций, чем любой другой менеджер паролей.

**LastPass**

Premium предлагает множество лучших функций, включая кроссплатформенную синхронизацию, безопасный обмен, отчет о надежности пароля и мониторинг даркнета. Однако изменение правил синхронизации устройств делает бесплатную версию LastPass практически бесполезной для большинства людей.

|  |  |  |
| --- | --- | --- |
| **Название** | **Плюсы** | **Минусы** |
| **Zoho Vault** | * Простота в использовании * Многофункциональная бесплатная версия * Многофакторная аутентификация (MFA) | * Устаревшие настольные приложения * Не удается автоматически заполнить некоторые типы персональных данных * Сайт взломан в 2015 году |
| **Dashlane** | * Простая синхронизация между устройств * Встроенный VPN * Мониторинг темной сети | * Ограничение на 50 паролей на бесплатном плане * Бесплатный план ограничен для использования на одном устройстве * Ограниченное облачное хранилище |
| **Bitwarden** | * Неограниченное количество паролей и синхронизация в бесплатной версии * Генератор безопасных паролей | * Некоторые проблемы с расширением браузера Edge * Ограниченная поддержка iOS * Безопасный обмен стоит дополнительно |
| **LogMeOnce Password Management Suite Ultimate** | * Кроссплатформенная поддержка * Зашифрованное хранилище * Легко настраиваемый | * Может быть сложным для новых пользователей * Дополнения дорогие |
| **LastPass** | * Поддерживает множество платформ и браузеров * Отчет о надежности пароля и инструменты мониторинга даркнета * Безопасный обмен и наследование паролей * Двухфакторная аутентификация | * Ограничения синхронизации для бесплатных пользователей * Некоторые типы персональных данных нельзя использовать для заполнения форм * Нет поддержки U2F * Некоторые компоненты содержат устаревшие параметры. |

**Вывод:** менеджер паролей должен быть простым в использовании, иметь достойную бесплатную версию, • Многофакторная аутентификация (MFA), быть кроссплатформенным, уметь генерировать надёжные пароли, легко настраиваться, предоставлять возможность хранения не только паролей, но и другой информации.

Существующие аналоги имеют гигантские базы пользователей с шифрованными данными, и, к сожалению, они не видят большую выгоду в обновлении уровней безопасности хранения данных. Чтобы поменять старые стандарты, которые были выбраны на этапе создания сервиса, придётся расшифровать абсолютно все пароли и логины, провести хэширование всех паролей заново, что займёт огромное количество времени и средств. Поэтому создание новой информационной системы гарантирует самый высший и современный способ защиты данных пользователей.

1.4 Составление проекта разрабатываемого продукта

1.4.1 Описание функциональных процессов

Функциональные процессы представляют собой совокупность всех действий информационная система должна выполнить, чтобы выполнить какую-либо функцию.

Функциональные процессы менеджера паролей:

* Вход пользователя
* Смена мастер-пароля
* Процесс создания аккаунта в системе
* Процесс добавления элемента
* Процесс выхода пользователя из системы

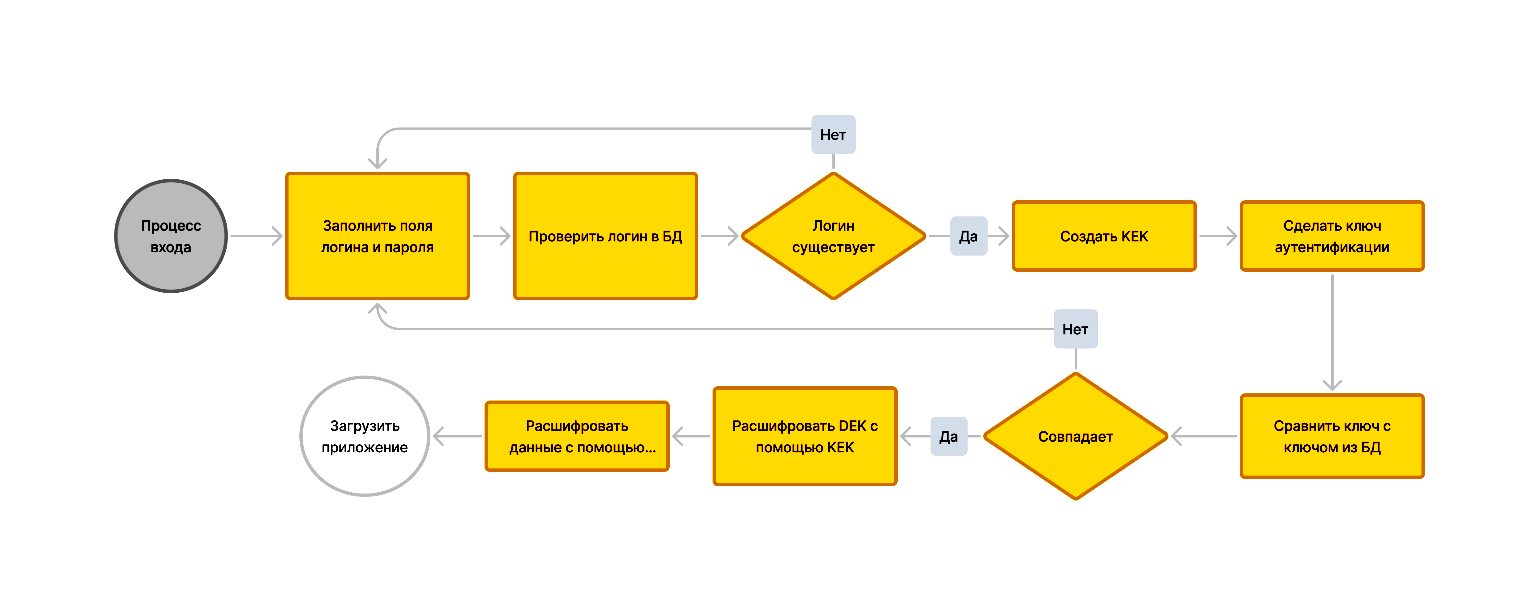


Рисунок 1. Процесс авторизации пользователя.

Процесс входа на рисунке 1 включает в себя проверку существования аккаунта с ведёнными пользователем данными и создание ключа аутентификации для входа в систему.

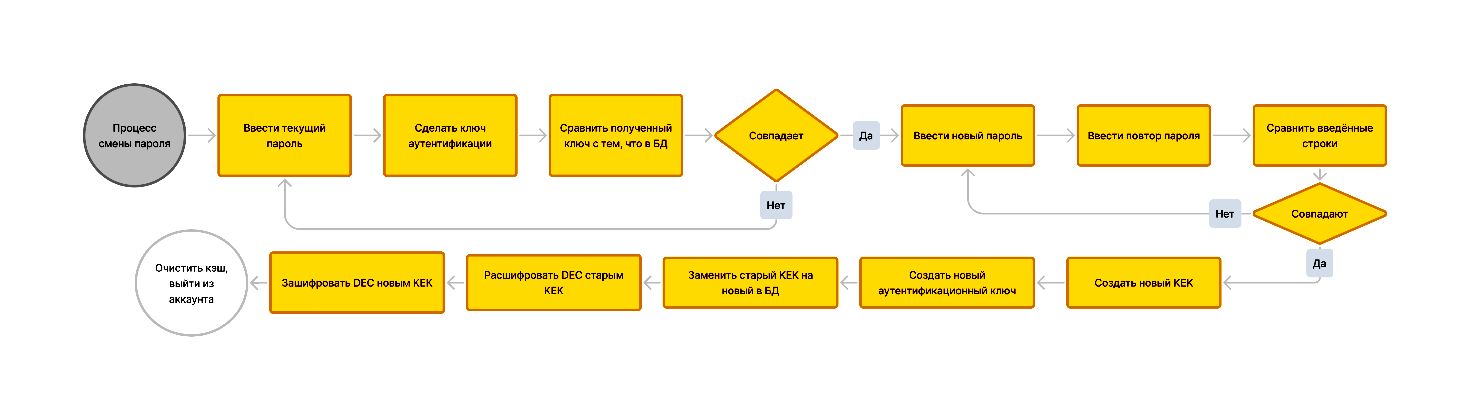


Рисунок 2. Смена мастер-пароля.

Процесс смены пароля на рисунке 2 включает в себя повторный процесс авторизации для удостоверения пользователя, что он владелец аккаунта, повторный процесс регистрации пользователя, в конце которого старые логин и пароль заменяются на новые в БД. По завершению вывести экран авторизации.

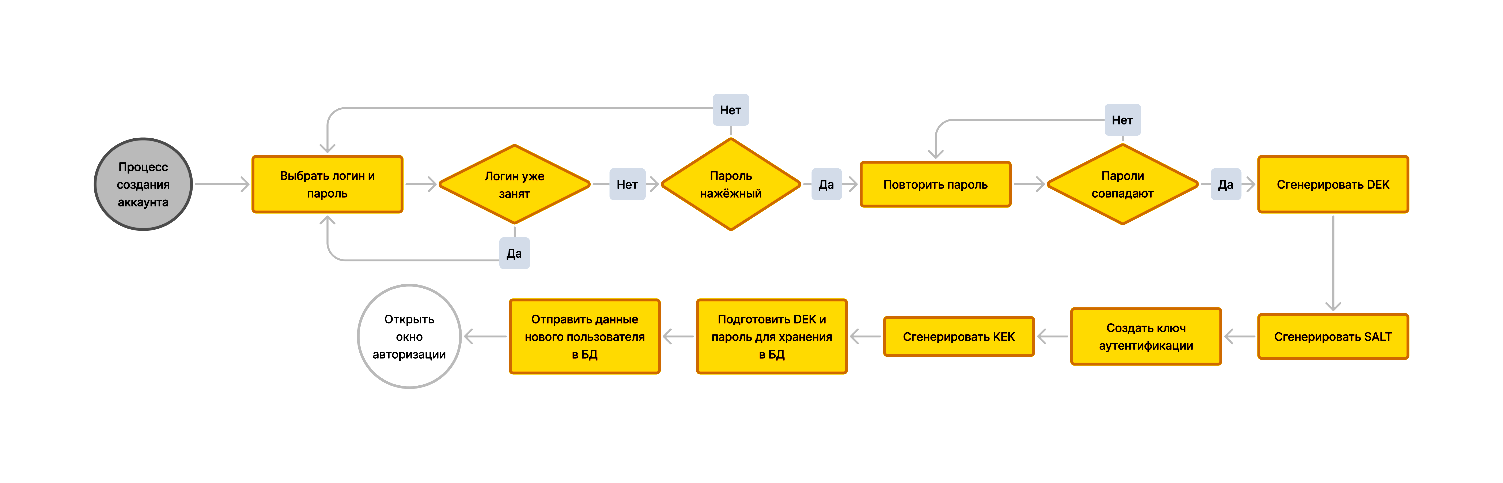


Рисунок 3. Процесс создания аккаунта в системе.

Процесс создания аккаунта на рисунке 3 включает в себя создание трёх ключей безопасности, созданных из ведённых пользователем данных, и загрузка в базу данных в качестве нового пользователя.

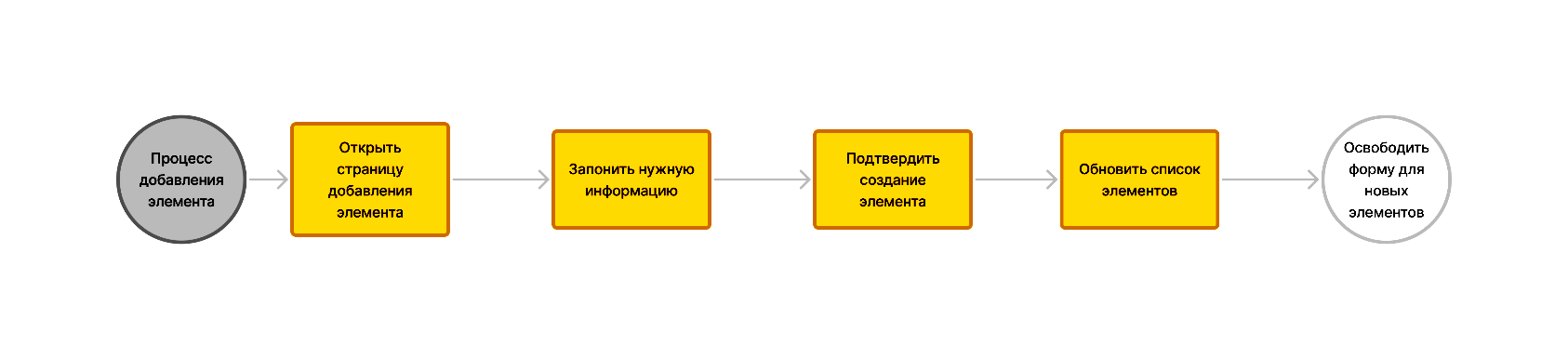


Рисунок 4. Процесс добавления элемента.

Процесс добавления элемента на рисунке 4 включает в себя простое добавление введённых данных в группу других элементов.

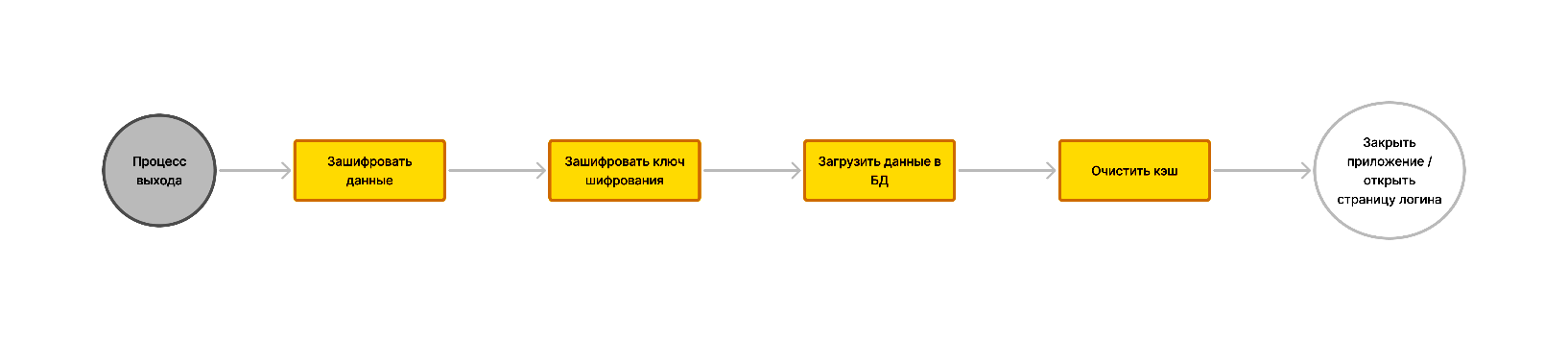


Рисунок 5. Процесс выхода пользователя из системы.

Процесс выхода пользователя из системы на рисунке 5 включает в себя зашифровка данных и отправка в базу данных, удаление всех паролей из оперативной памяти и переход на страницу входа (если пользователь вышел из аккаунта) или закрытие приложения (если пользователь закрыл менеджер паролей).

1.4.2 Проектирование базы данных

База данных менеджера паролей является очень важной частью работоспособности всей информационной системы, отвечающая за безопасность данных в состоянии покоя (Rest). Хотя это самое простое состояние для защиты от хакеров в сравнении с данными в использовании или в пути, именно базы данных являются наиболее частыми причинами утечек данных.

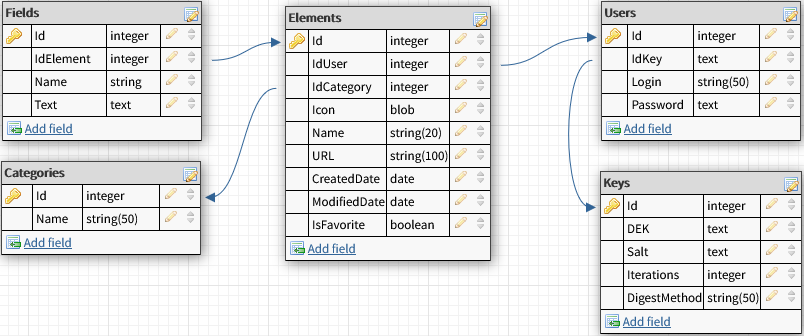


Рисунок 6. Спроектированная база данных для менеджера паролей.

База данных менеджера паролей на рисунке 6 включает в себя пять таблиц:

**Таблица Fields (Поля)**

Эта таблица содержит все данные элемента, которые пользователь хочет зашифровать. Эта таблица существует отдельно от другой с названием Elements по причине технологии, которая предоставляет возможность добавлять пользовательское число полей элемента, от минимума – одного поля до максимума – пяти полей. Тем самым снимается ограничение менеджера паролей хранить только пароли, то есть таким образом можно хранить любую текстовую информацию в зашифрованном виде.

Id – число, уникальный идентификационный номер;

IdElement – внешний ключ, по которому будет определяться к какому элементу какое поле принадлежит;

Name – название поля, которое существует для удобства пользователя, по которому он сможет быстро найти нужное поле;

Text – неограниченная строка для самой важной информации, такой как пароль.

**Таблица Categories (Категории)**

Для удобства пользования в менеджере паролей есть возможность группировать элементы по категории, чтобы пользователь смог быстро найти нужные ему данные.

Id – число, уникальный идентификационный номер;

Name – название категории, по которому пользователь будет фильтровать свой поиск.

**Таблица Elements (Элементы)**

Центральная таблица, хранящая информацию из других таблиц, чтобы собрать воедино данные об элементе. Элемент в менеджере паролей имеет привязку к пользователю и категории, иконку для быстрого визуального поиска в списке элементов, название и ссылка на сервис, к которому относятся данные из полей, даты создания и редактирования, логическая переменная «IsFavorite» для отдельной категории «Избранное», куда пользователь может добавить любые поля для быстрого доступа.

Id – число, уникальный идентификационный номер;

IdUser – внешний ключ, привязка к пользователю;

IdCategory – внешний ключ, привязка к категории;

Icon – blob, изображение (иконка сервиса);

Name – строка с лимитов в 20 символов, название сервиса;

URL – строка с лимитом в 100 символов, ссылка на сервис;

CreatedDate – дата, дата создания;

ModifiedDate – дата, дата редактирования;

IsFavorite – логическая переменная, входит ли элемент в категорию «Избранное».

**Таблица Users (Пользователи)**

Данная таблица отвечает за очень важный процесс – распределение элементов по пользователям, чтобы только необходимые элементы были показаны какому-то человеку. В таблице хранятся логин, который является помощником при входе, помогающий совершить быстрый поиск в базе данных, и пароль, что является ключом, который позволяет войти в систему и расшифровывает всё остальное в базе данных, относящееся к пользователю.

Id – число, уникальный идентификационный номер;

IdKey – внешний ключ, ссылку на очень важную таблицу, которая содержит дополнительные данные для расшифровки;

Login – строка с лимитом в 50 символом, уникальный, это псевдоним пользователя;

Password – неограниченная строка, содержит мастер-пароль.

**Таблица Keys (Ключи)**

В таблице лежит необходимые данные для расшифровки элементов, в которых мастер-пароль становится бесполезным.

Id – число, уникальный идентификационный номер;

DEK – неограниченный текст, Data Encryption Key, зашифрованный текст ключа шифрования данных;

Salt – неограниченный текст, произвольный набор символов, сгенерированный при регистрации пользователя;

Iterations – число, содержит число итераций, использованное при хешировании пароля;

DigestMethod – строка с лимитом в 50 символов, метод хеширования.

1.4.3 Макет и графический дизайн менеджера паролей

Макет и дизайн помогает определиться с графической темой приложения и инструментами для её осуществления на этапе анализа и проектирования. Это помогает ускорить процесс, а также отделить его от практической разработки, что может быть полезным при работе в команде.

Мы используем пароли каждый день, а значит дизайн менеджера паролей должен быть нейтральным, приспособленный для ежедневного использования. Достичь этого можно минимизировав количество окон, лёгкими и нейтральными цветами, меньшим количеством элементов.

Окна менеджера паролей:

* Окно авторизации
* Окно регистрации
* Окно с элементами
* Окно с настройками профиля
* Окно смены пароля

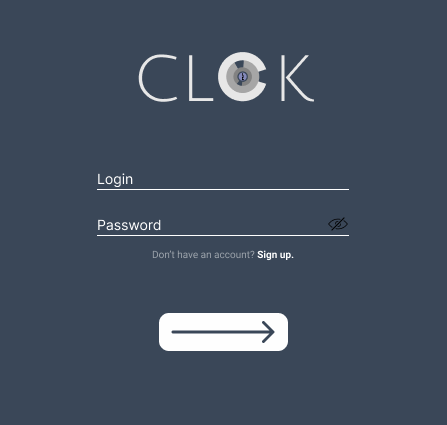


Рисунок 7. Окно авторизации пользователя.

Окно авторизации на рисунке 7 включает в себя стандартную форму заполнения логина и пароля, предлагая дополнительные опции в виде регистрации, если пользователь хочет создать аккаунт.



Рисунок 8. Окно регистрации пользователя.

Окно регистрации пользователя на рисунке 8 можно открыть через окно авторизации. Здесь можно создать новый аккаунт, а также посмотреть требования к паролю, которые хранятся в текстовом файле на файлах менеджера пароля. Есть кнопка назад, которая ведёт к окну авторизации, и вперёд, которая запускает процесс создания аккаунта в информационной системе.

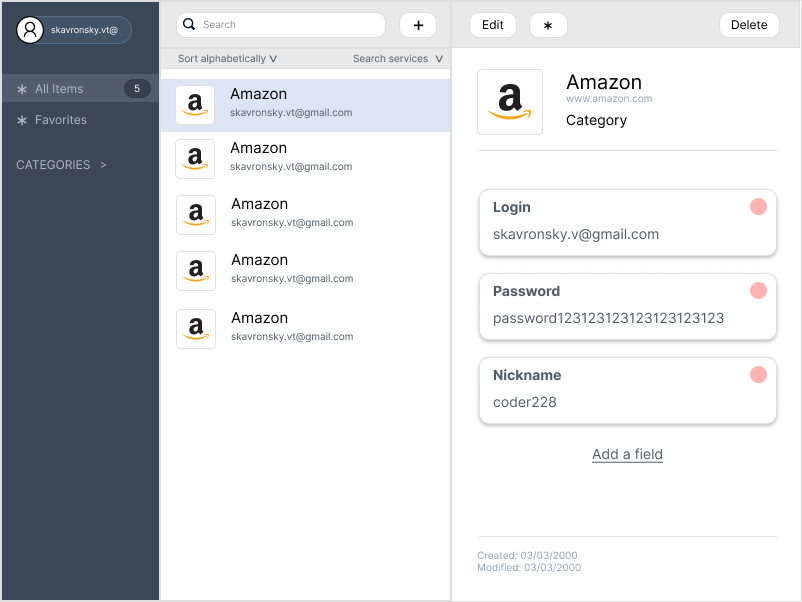


Рисунок 9. Окно элементов менеджера паролей.

Окно с элементами менеджера паролей на рисунке 9 содержит три части, представляющие путь к элементу: левая панель, которая служит навигацией между группами и категориями, средняя панель, зависящая от левой, содержит список элементов в выбранной группе, правая панель, зависящая от средней, содержит данные и формы по выбранному или создаваемому элементу.

Левая панель представляет из себя три кнопки, самая верхняя из которых ведёт к настройкам профиля, и одно древовидное меню (Categories), которое открывается по нажатию.

Средняя панель состоит из двух частей: панель поиска и список элементов. Панель поиска включает в себя строку поиска, кнопку добавления нового элемента, фильтры сортировки и поиска (по названию сервиса или по первому полю). Список элементов состоит из строк, представляющих один элемент. В неё входят иконка, название сервиса и значение первого поля.

Правая панель состоит двух частей: топ панель и данные о сервисе. Топ панель включает в себя кнопки управления элементом (редактировать, добавить в избранное, удалить элемент). Панель с данными о сервисе предлагает добавить или изменить иконку, название, ссылка сервиса, поля с их названием и содержимом.

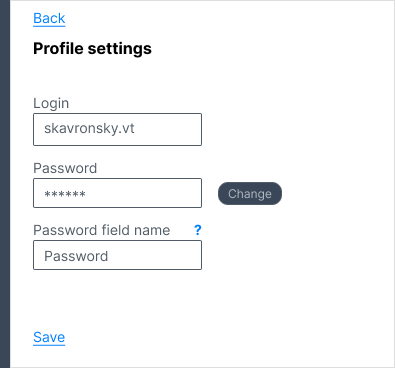


Рисунок 10. Окно настроек пользователя.

Окно с настройками профиля на рисунке 10 включает в себя кнопку навигации (Back), три поля для ввода новой информации, кроме пароля (второе поле «Password»), которое возможно поменять в окне смены пароля, на которое можно перейти по нажатию кнопки Change справа от поля.

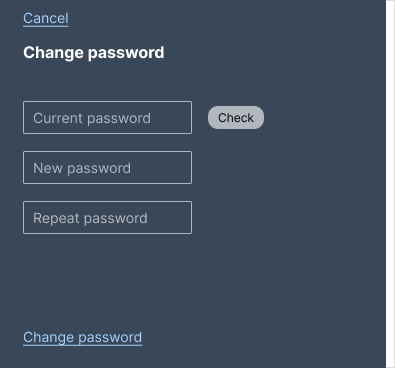


Рисунок 11. Окно смены пароля.

В окне смены пароля на рисунке 11 пользователь может поменять мастер-пароль после подтверждения текущего, что можно сделать, введя его в первое поле «Current password» и нажав на кнопку справа от поля «Check». Отменить или подтвердить выбор можно по первой и последней кнопкам «Cancel», «Change password».

1.5 Выбор инструментов и необходимых средств для реализации проектного решения

Для реализации менеджера паролей как информационную систему с графическим интерфейсом и зашифрованной базой данных, необходим ряд инструментов, которые помогут собрать из своих функций одно работающее приложение.

Понадобятся библиотеки и фремворки для следующих задач:

* + Создать оконное приложение,
  + Зашифровать базу данных,
  + Создать псевдослучайную строку,
  + Хэшировать данные,
  + Создать базу данных.

**Python**

Python — это язык программирования, который позволяет вам работать быстро и более эффективно интегрировать системы.

**PyQt5**

Qt — это набор кроссплатформенных библиотек C++, реализующих высокоуровневые API для доступа ко многим аспектам современных настольных и мобильных систем.

PyQt5 — это полный набор привязок Python для Qt v5. Он реализован в виде более чем 35 модулей расширения и позволяет использовать Python в качестве альтернативного языка разработки приложений для C++ на всех поддерживаемых платформах.

**SQLCipher**

SQLCipher — это библиотека с открытым исходным кодом, которая обеспечивает прозрачное и безопасное 256-битное шифрование AES для файлов базы данных SQLite.

**SQLite**

SQLite — это библиотека, которая реализует небольшой, быстрый, автономный, высоконадежный, полнофункциональный механизм базы данных SQL. SQLite — самая используемая СУБД в мире. SQLite встроен во все мобильные телефоны и большинство компьютеров и входит в состав бесчисленного множества других приложений, которые люди используют каждый день.

**Passlib**

Passlib — это библиотека хеширования паролей для Python, которая обеспечивает кроссплатформенные реализации более 30 алгоритмов хеширования паролей, а также платформу для управления существующими хэшами паролей. Он разработан, чтобы быть полезным для широкого круга задач, от проверки хэша до обеспечения хэширования паролей полной надежности для многопользовательских приложений.

**Secrets**

Модуль секретов используется для генерации криптографически стойких случайных чисел, подходящих для управления такими данными, как пароли, аутентификация учетной записи, токены безопасности и связанные с ними секреты. Он обеспечивает доступ к наиболее безопасному источнику случайности, который предоставляет операционная система.

Глава 2. Реализация менеджера паролей

2.1 Разработка составных элементов

Минимальное число элементов, необходимых для минимально работоспособной автоматизированной системы необходимо создать базу данных и способы общения пользователя с ней – пользовательский интерфейс.



2.1.1 Разработка базы данных

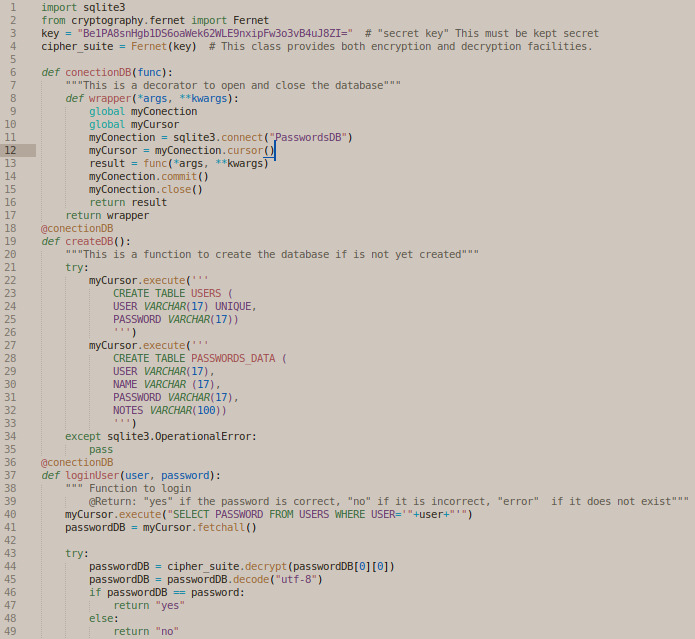


Рисунок 12. Создание таблицы в базе данных.

Первые строчки кода файла db.py на рисунке 12 проектируют базу данных, создавая столбцы и определяя ключ шифрования, с помощью которого будет работать cryptography. Далее выстраивается логика входа: если пользователь существует, то спрашивать корректный пароль, если нет, то создать нового.



Рисунок 13. Процессы в базе данных.

Методы на рисунке 13 контролируют изменения базы данных: добавить, изменить, прочитать.

2.1.2 Разработка приложения

В данном решении используется tkinter конструктор оконных приложений, так как он проще и быстрее для изучения, и подходит для такого типа проекта.

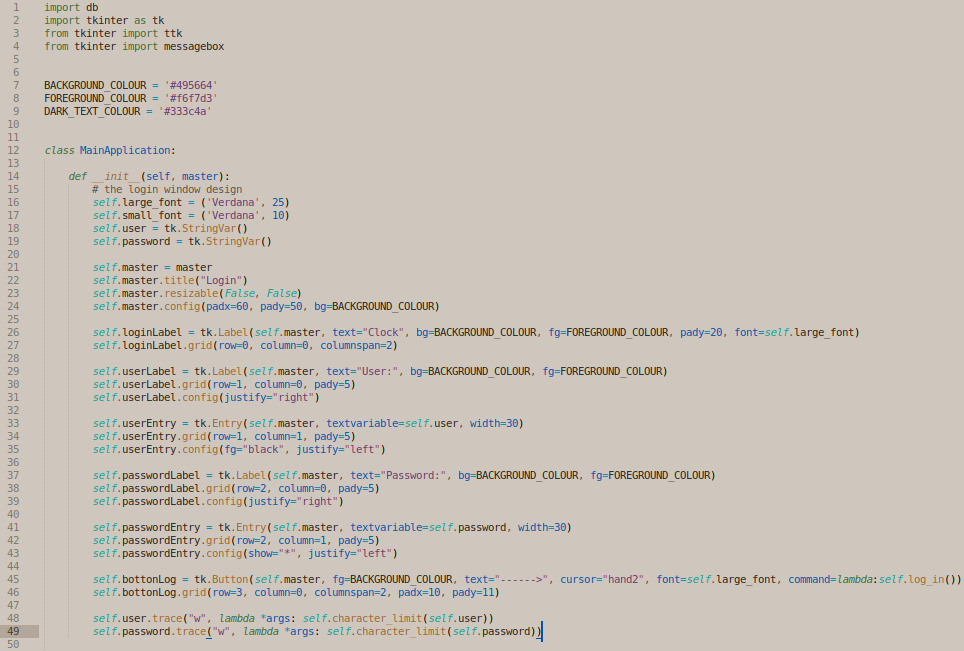


Рисунок 14. Начало главного файла приложения.

На рисунке 14 в начале импортированы нужные модули для работы всего приложения и база данных. Метод \_\_init\_\_ инициализирует запуск, выдаёт окно авторизации.



Рисунок 15. Процесс логина и регистрации, окно с элементами.

На рисунке 16 есть два метода, первый – log\_in, отвечает за процесс авторизации или регистрации. Второй – passwordStorageWindow, отвечает за построение окна элементов

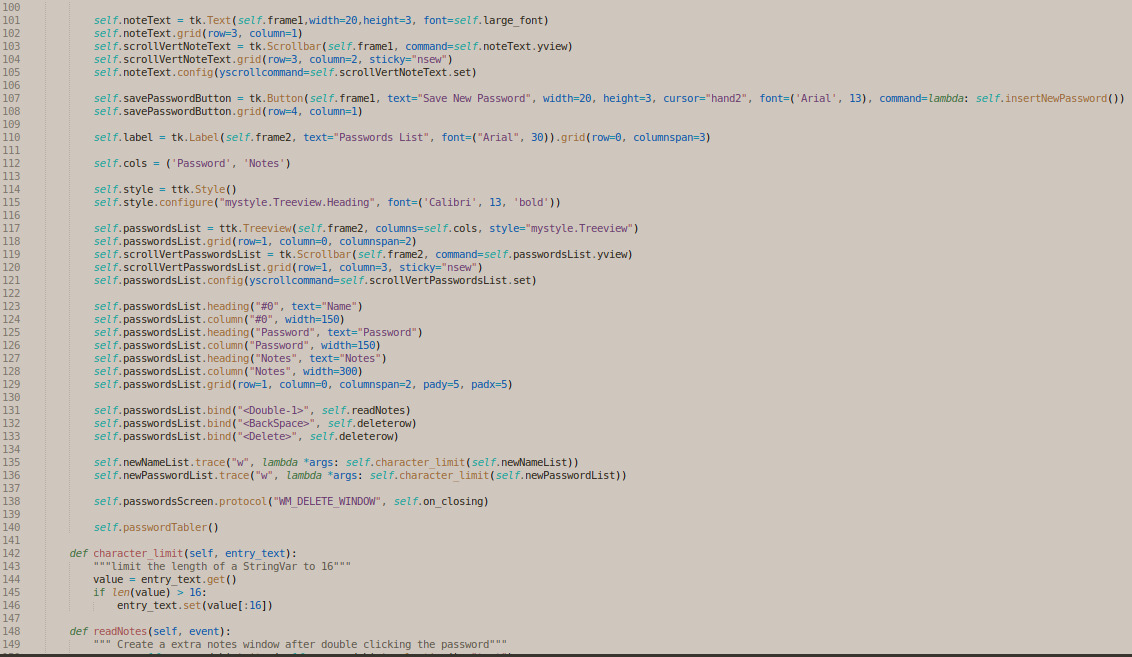


Рисунок 16. Генерация таблицы с данными пользователя.

На рисунке 16 написана таблица, в которую выводятся данные пользователя: имя сервиса, пароль, заметки.

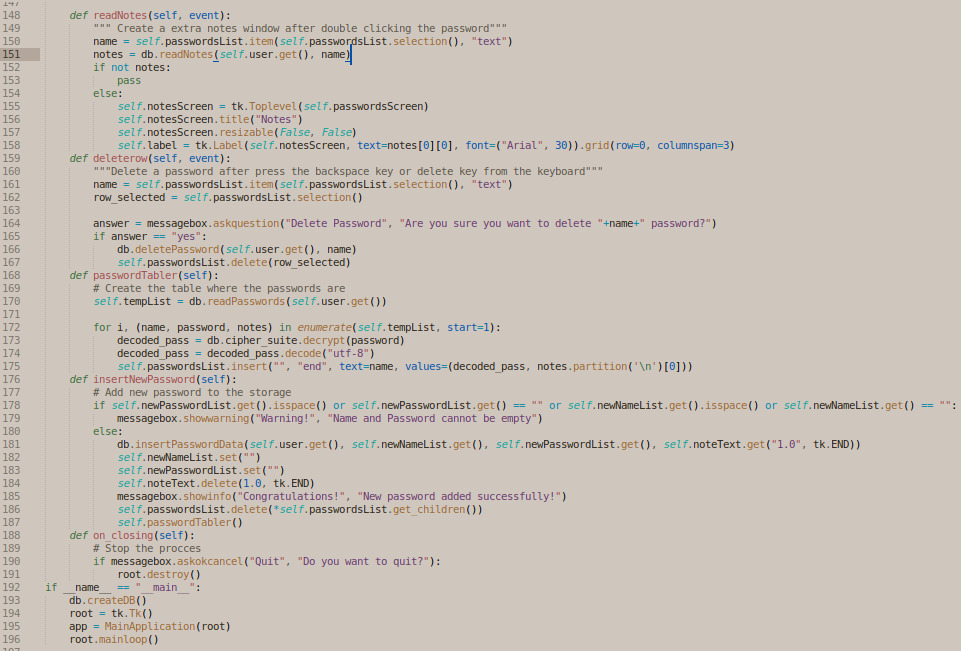


Рисунок 17. Процессы, связанные с таблицей.

На рисунке 17 прописаны функции, которые пользователь может использовать: удалить пароль, добавить пароль, открыть заметки. Некоторые вспомогательные методы для загрузки данных в таблицу.

2.2 Монтаж установка и настройка

Для работы информационной системы необходим ряд дополнительных библиотек, устанавливающихся отдельно. Благодаря языку программирования Python, получить доступ ко всем нужным файлам иожно через команду pip. Все они хранятся в облаке, то есть нужен доступ в сеть, и скачать их можно при помощи команды.

**sudo apt install sqlite3** – установить инструменты базы данных.

**pip install cryptography –** установить инструменты шифрования.

**sudo apt install sqlcipher –** установить инструменты шифрования базы данных.

**pip install secrets** – установить secrets

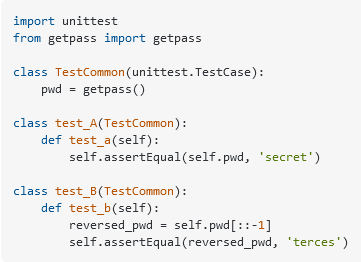
**pip install passlib** – установить passlib

После ввода этих команд, приложение готова к запуску и нормальной работе.

2.3 Тестирование, ввод в эксплуатацию

Одна из важных проверок в менеджере паролей – то, что нежеланные лица не смогут получить доступ к данным другого человека.

Для проверки процесса входа был применен инструмент unittest, встроенные в язык программирования Python. Он позволяет проводит пользовательские тесты, что означает, он подходит во множестве случаев, включая этот.



2.4 Разработка сопроводительной документации

Если вы еще не создали учетную запись, попробуйте войти в систему с нужной учетной записью, и если она еще не используется, вы сможете ее создать.

Чтобы удалить один пароль, просто выберите его и нажмите клавишу Backspace или удалите с клавиатуры.

Чтобы просмотреть полные примечания к паролю, дважды щелкните соответствующий пароль.

Заключение

По завершению ознакомления с предметной область проекта, можно приобрести цельную картину об устройстве современного цифрового мира, в котором пользователи ежедневно хранят, используют и передают данные, некоторые из которых чрезвычайно личные, не созданные для посторонних глаз, и очень важно держать такую информацию в безопасности.

Её обеспечивают алгоритмы шифрования, работающие с помощью секретной фразы под название password или passphrase. Эта самая важный секрет, без которого всё останое становится доступным в открытом виде.

Хотя технологии обещают облегчить нашу жизнь, и, как правило, так оно и есть, каждый новый веб-сайт и приложение, на которые мы подписываемся, - это еще один пароль, который мы должны запомнить. Для большинства из них стало невозможным запомнить их все. При создании новой учетной записи веб-сайты требуют, чтобы мы создавали длинные и надежные пароли. В противном случае нам даже не разрешат создать учетную запись. Предполагая, что вы пройдете этап создания учетной записи, вы быстро забудете шифр, который вы только что создали, и смиритесь с использованием “Забыли пароль?” ссылка в качестве опции для ежедневного входа в систему.

Решение является интересным и успешным методом исправления этой проблемы – менеджер паролей.

У менеджера паролей одна главная, но очень важная задача – сохранить данные пользователя в безопасности. Для этого были созданы и применяются различные способы, от простых и известных с давних времён (пароль), до современных и только становящихся стандартным инструментом защиты информации, таких как двух факторная аутентификация и биометрические данные, т. е. лицо или отпечаток владельца.

Список используемых источников

1. PCMag: Компьютерный журнал: [сайт]. – Сравнение менеджеров паролей – URL: <https://www.pcmag.com/picks/the-best-password-managers> (дата обращения: 26.03.2022). - Текст : электронный.
2. StackExchange: сеть веб-сайтов для работы с вопросами и ответами в различных областях: [сайт]. – Как работает шифрование в БД – URL: <https://www.pcmag.com/picks/the-best-password-managers> (дата обращения: 26.03.2022). - Текст : электронный.
3. Investopedia: Компьютерный журнал: [сайт]. - Сравнение менеджеров паролей - URL: <https://www.investopedia.com/best-password-managers-5080381> (дата обращения: 26.06.2018). - Текст : электронный.
4. Wikipedia : электронная энциклопедия : [сайт]. - Что такое CSPRNG - URL: <https://en.wikipedia.org/wiki/Cryptographically-secure_pseudorandom_number_generator> (дата обращения: 26.06.2018). - Текст : электронный.
5. PBKDF2 : официальный сайт : [сайт]. - Что такое PBKDF2 - URL: <https://www.pbkdf2.com/> (дата обращения: 26.06.2018). - Текст : электронный.
6. Wikipedia : электронная энциклопедия: [сайт]. - Что такое PBKDF2 - URL: <https://en.wikipedia.org/wiki/PBKDF2> (дата обращения: 26.06.2018). - Текст : электронный.
7. Cryptobook.nakov: криптография для разработчиков: [сайт]. - Что такое PBKDF2 - URL: <https://cryptobook.nakov.com/mac-and-key-derivation/pbkdf2> (дата обращения: 26.06.2018). - Текст : электронный.
8. Wikipedia : электронная энциклопедия: [сайт]. - Что такое SALT - URL: <https://en.wikipedia.org/wiki/Salt_(cryptography)> (дата обращения: 26.06.2018). - Текст : электронный.
9. Youtube: видео хостинг : [сайт]. - Как менеджеры паролей работают - URL: <https://www.youtube.com/watch?v=w68BBPDAWr8> (дата обращения: 26.06.2018). - Текст : электронный.
10. Youtube : видео хостинг: [сайт]. - Как хранить пароли в базе данных - URL: <https://www.youtube.com/watch?v=8ZtInClXe1Q> (дата обращения: 26.06.2018). - Текст : электронный.
11. Youtube: видео хостинг: [сайт]. - Базовые концепты криптографии - URL: <https://www.youtube.com/watch?v=NuyzuNBFWxQ> (дата обращения: 26.06.2018). - Текст : электронный.
12. Youtube: видео хостинг: [сайт]. - Public key Encryption - URL: <https://www.youtube.com/watch?v=GSIDS_lvRv4> (дата обращения: 26.06.2018). - Текст : электронный.
13. Youtube: видео хостинг: [сайт]. - Public key Encryption - URL: <https://www.youtube.com/watch?v=NmM9HA2MQGI> (дата обращения: 26.06.2018). - Текст : электронный.

Youtube: видео хостинг: [сайт]. - Public key Encryption - URL: <https://www.youtube.com/watch?v=AQDCe585Lnc> (дата обращения: 26.06.2018). - Текст : электронный.

1. Youtube: видео хостинг: [сайт]. - Public key Encryption - URL: <https://www.youtube.com/watch?v=6-JjHa-qLPk> (дата обращения: 26.06.2018). - Текст : электронный.
2. TAdviser : портал выбора технологий и поставщиков: [сайт]. - Кибератаки - URL: <https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8> (дата обращения: 26.06.2018). - Текст : электронный.
3. Wikipedia : электронная энциклопедия: [сайт]. - Что такое пароль - URL: <https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C> (дата обращения: 26.06.2018). - Текст : электронный.
4. JDLT : ИТ-услуги и ИТ-консалтинг: [сайт]. - Требования к надёжному паролю в 2022 году - URL: <https://jdlt.co.uk/blog/password-security-in-2022/> (дата обращения: 26.06.2018). - Текст : электронный.
5. Cybernews : источник последних новостей кибербезопасности и независимых исследований: [сайт]. - Безопасность менеджеров паролей в 2022 - URL: <https://cybernews.com/best-password-managers/are-password-managers-safe/> (дата обращения: 26.06.2018). - Текст : электронный.
6. Techtarget : медиа-ресурс специально для покупателей корпоративных технологий: [сайт]. - Как защитить данные пока они хранятся, используются или передаются - URL: <https://www.techtarget.com/searchsecurity/feature/Best-practices-to-secure-data-at-rest-in-use-and-in-motion> (дата обращения: 26.06.2018). - Текст : электронный.
7. Wikipedia : электронная энциклопедия : [сайт]. - Role-based access control - URL: <https://en.wikipedia.org/wiki/Role-based_access_control> (дата обращения: 26.06.2018). - Текст : электронный.
8. SecureDataRecovery : доверенный орган восстановления RAID, SSD и жесткого диска: [сайт]. - Необходимость надёжных паролей - URL: <https://www.securedatarecovery.com/resources/the-importance-of-strong-secure-passwords> (дата обращения: 26.06.2018). - Текст : электронный.