**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА**

Факультет прикладної математики та інформатики

(повне найменування назва факультету)

Кафедра дискретного аналізу та інтелектуальних систем

(повна назва кафедри)

**КУРСОВА РОБОТА**

РОЗРОБКА КОМП’ЮТЕРНОЇ ПРОГРАМИ ДЛЯ МЕНЕДЖМЕНТУ ТА ГЕНЕРАЦІЇ ПАРОЛІВ “SecurePass”

Виконав: студент групи ПМІ-33

спеціальності 122 – Комп’ютерні науки

(шифр і назва спеціальності)

Тимчишин Я. А.

(підпис) (прізвище та ініціали)

Керівник Стойко Т. І.

(підпис) (прізвище та ініціали)

2024

**ЗМІСТ**

[ВСТУП 1](#_Toc167812962)

[Актуальність тематики 1](#_Toc167812963)

[Мета і важливість роботи 1](#_Toc167812964)

[РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ SECUREPASS 3](#_Toc167812965)

[1.1. Огляд існуючих методів менеджменту паролів 3](#_Toc167812966)

[1.2. Переваги та недоліки існуючих програм 7](#_Toc167812967)

[1.3. Переваги SecurePass над іншими програмами 11](#_Toc167812968)

[РОЗДІЛ 2. ОСНОВНІ ТЕХНОЛОГІЇ РОЗРОБКИ SECUREPASS 13](#_Toc167812969)

[РОЗДІЛ 3. ІНТЕРФЕЙС ТА ОСНОВНА РОБОТА ПРОГРАМИ 22](#_Toc167812970)

[ВИСНОВКИ 32](#_Toc167812971)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 33](#_Toc167812972)

# ВСТУП

# Актуальність тематики

В сучасному світі, де кожен з нас регулярно користується безліччю онлайн-сервісів, питання безпеки паролів стає все більш важливим. Кожен користувач має десятки, а то й сотні паролів для доступу до своїх електронних поштових скриньок, банківських рахунків, соціальних мереж, онлайн-магазинів, різних додатків та інших онлайн-платформ.

Запам’ятати усі ці паролі навряд чи під силу будь-якій пересічній людині, а використання однакових паролів для різних сервісів або платформ не є хорошою ідеєю. Це власне є найгіршою ідеєю, яка тільки може прийти в голову, адже в разі витоку одного із паролів, під загрозою також опиняться й усі інші акаунти, сервіси або платформи, на яких використовується цей пароль.

У зв’язку з цим надзвичайно актуальною стає потреба у використанні надійних інструментів для менеджменту паролів. Програма SecurePass, яку буде розроблено в рамках цієї курсової роботи, покликана забезпечити користувачам зручний та безпечний інтсрумент для зберігання, генерації та керування їхніми паролями.

# Мета і важливість роботи

Метою цієї курсової роботи є розробка та дослідження десктопної програми SecurePass для менеджменту та генерації паролів, яка буде забезпечувати користувачам зручний інтерфейс, високий рівень безпеки та широкий спектр функцій.

Ця десктопна програма буде мати значний вплив на користувачів, пропонуючи їм ряд переваг:

* **Забезпечення безпечного зберігання паролів:** SecurePass використовуватиме надійні методи шифрування та хешування для захисту паролів від несанкціонованого доступу, навіть у разі витоку бази даних, що значно знижуватиме ризик злому онлайн-акаунтів, крадіжки особистих даних та фінансового шахрайства.
* **Додавання, видалення, редагування та структурування паролів по папках:** SecurePass матиме зручний та зрозумілий інтерфейс для управління паролями, який дозволить легко і просто додавати нові паролі, видаляти застарілі, редагувати існуючі та структурувати паролі по тематичних папках для кращої організації.
* **Генерація хороших та надійних паролів:** SecurePass матиме вбудований генератор паролів, який даватиме змогу користувачеві створювати сильні та унікальні паролі для кожного сервісу, відповідно до поставлених користувачем вимог.
* **Додатковий функціонал:** SecurePass матиме додаткові функції, такі як сканер паролів, який регулярно перевірятиме всі збережені паролі користувача на наявність слабких місць, застарілих комбінацій та повторного використання. Це допоможе користувачам індентифікувати потенційно вразливі паролі та вжити заходів для їх посилення. Окрім сканера, також буде можливість змінювати мову інтерфейсу програми.
* **Авторизація користувачів за допомогою логіна та пароля:** SecurePass використовуватиме надійну систему аутентифікації для захисту доступу до сховища паролів. Користувачі будуть мати змогу створити унікальний логін та пароль, які будуть використовуватися для входу в систему та доступу до своїх паролів.
* **Зручний та інтуїтивно зрозумілий інтерфейс користувача:** SecurePass буде розроблений з урахуванням простоти використання та зручності навігації. Інтерфейс користувача буде зрозумілим навіть для недосвідчених користувачів, роблячи процес управління паролями максимально комфортним.

Все це буде особливо корисним та важливим для користувачів, які використовують багато онлайн-сервісів; користувачів, які мають проблеми із запам’ятовуванням усіх своїх паролів; та для користувачів, які стурбовані безпекою своїх онлайн-акаунтів.

# РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ SECUREPASS

# Огляд існуючих методів менеджменту паролів

На даний момент, існує досить небагато методів керування паролів. Деякі з них кращі зі інші, деякі – гірші. Далі ми розглянемо три найпопулярніші методи менеджменту паролів.

Найпростішим і найменш надійним методом, з усіх, що тільки можна придумати, є запам’ятовування паролів.

Звісно, людина сама по собі безперечно є справжнім дивом природи. Наше тіло – це неймовірно складна система, що складається з мільярдів клітин, які працюють злагоджено, виконуючи безліч функцій. Кожен орган нашого тіла володіє унікальними властивостями, і наш мозок – це, мабуть, найдивовижніший орган з усіх. Він важить лише близько 1.5 кілограма, але за складністю й потужністю перевершує будь-який комп’ютер, створений людиною. Мозок має близько 100 мільярдів нейронів, кожен з яких з’єднаний з тисячами інших, утворюючи неймовірно складну мережу. Завдяки цій мережі, людина спроможна на багато чого, включаючи здатність запам’ятовувати та зберігати близько 2.5 мільйонів гігабайт цифрової пам’яті, що є неймовірно надзвичайним[1].

Проте, навіть із здатністю запам’ятовувати стільки інформації, людині навряд чи вдасться запам’ятати усі свої складні та унікальні паролі до кожного зі своїх сервісів чи акаунтів, що в свою чергу часто призводить до використання простих, ненадійних та повторюваних комбінацій. А такі паролі легко піддаються підбору зловмисниками та хакерами. Якщо ж все-таки людині вдалося придумати якийсь складний пароль, з часом вона може його призабути, зробити помилку при введенні цього паролю і заблокувати свій же акаунт.

До прикладу, візьмемо ситуацію, яка сталася із одним німецьким програмістом Штефаном Томасом. У 2012 році він отримав 7 002 біткоїни в якості оплати за створення відеоролика, що пояснює, як працює криптовалюта. На той час ці біткоїни коштували лише кілька доларів за штуку. Однак, якщо перемотати час до сьогодення, кожен біткоїн оцінюється приблизно в 65 000 доларів США, що є досить великою сумою грошей. Томас зберігав усі свої біткоїни в цифровому гаманці IronKey на жорсткому диску. Щоб не забути пароль, він записав його на аркуші паперу. Але, на жаль, цей папірець зник, а сам пароль Штефан забув, і тепер він лишився без доступу до своїх цифрових статків.

Все би було не так погано, якби можна було безліч разів пробувати вгадати пароль до гаманця, підбираючи різні комбінації. Але гаманець, на якому зберігаються усі ці біткоїни, дозволяє лише десять спроб введення паролю. Якщо усі десять спроб невірні, гаманець шифрується, роблячи його назавжди недоступним. Томас вже вісім разів намагався вгадати невловимий код, але безуспішно. За його словами, він змирився з тим, що забув свій пароль, і визнав, що його цифрові статки можуть вже назавжди залишитися недосяжними[2].

Ця історія – це яскравий приклад, чому банальне запам’ятовування своїх паролів або ж використання випадкового аркуша для збереження паролю може призвести до дуже неприємних наслідків.

Ще одним досить-таки примітивним методом менеджменту та зберігання паролів є використання однакових паролів для усіх своїх сервісів та акаунтів.

Ця практика є надзвичайно небезпечною з очевидних причин, проте, незважаючи на це, досить поширеною поміж великої кількості людей. Це можна пояснити нерозсудливістю, необачністю або ж лінивістю людини. Використання однакових паролів може створювати ілюзію безпеки, адже вам здається, що ви створили і запам’ятали лише один пароль, який є надзвичайно складним та неповторним і ніхто інший за жодних обставин не зможе зламати. Проте насправді ця практика робить вас, навпаки, більш вразливими до хакерських атак.

Уявимо наступну ситуацію. Ви використовуєте один і той же пароль для усіх ваших акаунтів та сервісів: для електронної поштової скриньки, для банківського рахунку, для онлайн-магазину, для випадкового сайту, на якому ви зареєструвалися, щоб мати змогу дивитися різні кулінарні рецепти. Тепер скажемо, що відбулася хакерська атака на цей самий сайт з рецептами, і ваш пароль опинився в руках зловмисників. Перш ніж ви це усвідомите, зловмисник, використовучи пароль, який ви ввели при реєстрації на сайті і який використовується на усіх ваших інших акаунтах, зможе отримати доступ до усіх ваших персональних даних, ваших грошей та іншої вразливої інформації. Відбудеться так званий ефект метелика, коли найменша зміна призводить до великих наслідків. У цьому випадку, найменший витік даних – вашого паролю – призведе до втрати по суті усіх ваших даних. Саме тому не рекомендується використовувати один і той самий пароль для усіх ваших сервісів та акаунтів.

Наступним методом зберігання та управління паролями, безперечно кращим та надійнішим за попередні, є використання менеджерів паролів.

Менеджери паролів – це програмне забезпечення, яке допомагає користувачеві безпечно зберігати, організовувати та використовувати паролі. Вони пропонують ряд переваг, які роблять їх більш надійним і зручним способом менеджменту паролів.

Ось деякі із переваг:

* **Централізоване зберігання:** всі паролі зберігаються в одному місці в зашифрованому вигляді, що робить їх більш захищеними від несанкціонованого доступу. Це економить час і зусилля користувача, адже не потрібно запам’ятовувати кожен пароль окремо.
* **Генерація складних паролів:** Менеджери паролів можуть генерувати для користувача унікальні та надійні паролі, які відповідають найкращим практикам кібербезпеки. Це гарантує, що паролі будуть стійкими до кібер атак та різних методів злому.
* **Зручне керування:** Більшість менеджерів паролів пропонують зручний інтерфейс для керування паролями. Користувач може легко додавати, редагувати, видаляти та організовувати паролі за папками або різними категоріями.
* **Синхронізація на різних пристроях:** Багато менеджерів паролів пропонують синхронізацію між пристроями користувача, щоб користувач міг мати доступ до своїх паролів з будь-якого місця. Це робить їх зручними для використання на комп'ютерах, смартфонах та планшетах.
* **Додаткові функції:** Деякі менеджери паролів пропонують додаткові функції, такі як:
  + **Сканер паролів:** Перевіряє ваші паролі на надійність та виявляє слабкі, повторювані або компрометовані паролі.
  + **Двофакторна автентифікація:** Додає додатковий рівень безпеки до ваших акаунтів, вимагаючи введення коду з вашого телефону або іншого пристрою окрім пароля.
  + **Резервне копіювання та відновлення:** Забезпечує можливість відновлення ваших паролів у разі втрати пристрою або пошкодження даних.
  + **Автоматичний вхід:** Автоматично заповнює поля входу на веб-сайтах та програмах, що значно економить час та спрощує доступ до ваших акаунтів. Вам не потрібно вводити паролі вручну, що знижує ризик помилок та випадкового розкриття даних.

Окрім переваг, також можна згадати про кілька недоліків менеджерів паролів. А саме:

* **Залежність від програмного забезпечення:** Безпека ваших паролів залежить від надійності та стійкості до атак самого менеджера паролів, який ви використовуєте.
* **Вартість:** Деякі менеджери паролів пропонують безкоштовні тарифи з обмеженими функціями, а для доступу до всіх можливостей може знадобитися платна підписка.
* **Складність налаштування:** Первинне налаштування менеджера паролів може здатися складним для деяких користувачів.

Загалом, можна зробити висновок, що використання менеджера паролів є значно безпечнішим та зручнішим способом менеджменту паролів порівняно із запам’ятовуванням або використанням однакових паролів для різних сервісів. І хоча існують деякі недоліки, такі як залежність від програмного забезпечення або складність налаштування, переваги менеджерів паролів значно переважають над недоліками.

# Переваги та недоліки існуючих програм

Тепер коли ми знаємо, що менеджери паролів це цінний інструмент для керування своїми паролями, давайте розглянемо три уже реалізовані менеджери паролів, проаналізуємо безпеку кожної програми та оцінимо зручність їх використання.

* **1Password**

**Функціонал:**

* + Підтримка платформ: Windows, macOS, Linux, iOS, Android, веб-браузери.
  + Синхронізація: хмарна синхронізація через 1Password сервери.
  + Додаткові функції: сканер паролів, двофакторна автентифікація, автозаповнення форм, безпечний обмін паролями, віртуальний приватний сервер (VPN), Travel Mode (офлайн-доступ до паролів), Watchtower (попередження про компрометацію паролів).

**Безпека:**

* + Зберігання паролів: зашифроване локальне зберігання та хмарне зберігання з використанням AES-256, zero-knowledge.
  + Шифрування: end-to-end, ключ шифрується та зберігається на стороні клієнта.

**Зручність використання:**

* + Інтерфейс: інтуїтивно зрозумілий, елегантний, доступний в декількох мовах, зручний для початківців.
  + Безкоштовний план: недоступний, але доступна 14-денна безкоштовна пробна версія.

**Переваги:**

* + Високий рівень безпеки з використанням zero-knowledge та end-to-end шифрування.
  + Зручний та інтуїтивно зрозумілий інтерфейс.
  + Широкий спектр додаткових функцій, включаючи VPN.
  + Доступність на різних платформах.

**Недоліки:**

* + Відсутність безкоштовного тарифного плану з повним набором функцій.
  + Немає можливості локального резервного копіювання.
* **NordPass**

**Функціонал:**

* + Підтримка платформ: Windows, macOS, Linux, iOS, Android, веб-браузери.
  + Синхронізація: хмарна синхронізація через NordPass сервери.
  + Додаткові функції: сканер паролів, двофакторна автентифікація, плагіни для браузерів, автозаповнення форм, безпечний обмін паролями, генератор паролів.

**Безпека:**

* + Зберігання паролів: зашифроване локальне зберігання та хмарне зберігання з використанням AES-256, zero-knowledge.
  + Шифрування: end-to-end, де тільки користувач володіє ключем.

**Зручність використання:**

* + Інтерфейс: простий, лаконічний, доступний в декількох мовах, зручний для початківців.
  + Безкоштовний план: доступний, проте з обмеженими функціями, платний тариф для розширення функціоналу.

**Переваги:**

* + Високий рівень безпеки з використанням zero-knowledge та end-to-end шифрування.
  + Зручний та інтуїтивно зрозумілий інтерфейс.
  + Доступність безкоштовного тарифу.
  + Додаткові функції, такі як сканер паролів та генератор паролів.
  + Доступність на різних платформах.
  + Інтеграція з різними браузерами та програмами.

**Недоліки:**

* + Деякі функції, такі як сканер паролів, доступні лише у платній підписці.
  + Проблеми з інтеграцією в різних браузерах та на різних платформах.
  + Залежність від хмарної синхронізації для деяких функцій.
* **KeePassXC**

**Функціонал:**

* + Підтримка платформ: Windows, macOS, Linux, iOS, Android, веб-браузери.
  + Синхронізація: локальне зберігання через файли KeePassXC, синхронізація через хмарні сервіси або USB-накопичувачі.
  + Додаткові функції: сканер паролів, генератор паролів, плагіни для браузерів, автозаповнення форм, імпорт паролів з інших менеджерів.

**Безпека:**

* + Зберігання паролів: зашифроване локальне зберігання з використанням AES-256.
  + Шифрування: end-to-end шифрування, шифрування на стороні клієнта.

**Зручність використання:**

* + Інтерфейс: відкритий код, проте може видатися досить складним для розуміння та навігації.
  + Безкоштовний план: доступний.

**Переваги:**

* + Відкритий код, що гарантує прозорість та безпеку.
  + Безкоштовний тарифний план з повним функціоналом.

**Недоліки:**

* + Відсутність автоматичної синхронізації між пристроями без додаткових сервісів.
  + Менш привабливий та складніший інтерфейс порівняно з іншими менеджерами паролів.
  + Більш складне налаштування та використання порівняно з хмарними менеджерами паролів.

Кожен з розглянутих менеджерів паролів має свої переваги та недоліки. Нижче наведена таблиця, яка досить зрозуміло підсумовує порівняння цих трьох програм-менеджерів паролів:

|  |  |  |  |
| --- | --- | --- | --- |
| Функція | 1Password | NordPass | KeePassXC |
| Підтримка платформ | Windows, macOS, Linux, iOS, Android,  веб-браузери | Windows, macOS, Linux, iOS, Android,  веб-браузери | Windows, macOS, Linux, iOS, Android,  веб-браузери |
| Синхронізація | Хмарна | Хмарна | Локальна або хмарна (через сторонні сервіси) |
| Додаткові функції | Сканер паролів, 2FA, VPN, автозаповнення форм, безпечний обмін паролями | Сканер паролів, 2FA, генератор паролів, автозаповнення форм, безпечний обмін паролями, веб-плагіни | Сканер паролів, генератор паролів, автозаповнення, імпорт/експорт паролів,  веб-плагіни |
| Безпека | zero-knowledge, end-to-end шифр,  AES-256 | zero-knowledge, end-to-end шифр,  AES-256 | Відкритий код, AES-256 |
| Зручність використання | Інтуїтивний інтерфейс | Простий інтерфейс | Менш простий інтерфейс |
| Безкоштовний тариф | Ні | Так (обмежений функціонал) | Так |

# Переваги SecurePass над іншими програмами

Розроблена програма SecurePass пропонуватиме користувачам комбінацію високого рівня безпеки, зручного інтерфейсу та розширених функцій, що робитиме його чудовим вибором для всіх, хто шукає надійний менеджер паролів.

SecurePass буде доступний для всіх зацікавлених користувачів операційної системи Windows. Поки що, він буде доступний лише в десктопній версії, що забезпечуватиме високу продуктивність та інтеграцію з цією оперативною системою. Десктопна версія не буде залежати від роботи інтернету, що робитиме її більш надійною та стійкою до збоїв. Також ця версія SecurePass гарантуватиме максимальну конфіденційність, оскільки ваші паролі ніколи не покидають ваш комп’ютер.

SecurePass не залежатиме від жодних хмарних сервісів, що надасть вам повний контроль над вашими паролями та гарантуватиме, що ваші дані не будуть доступні стороннім особам. Усі ваші паролі зберігатимуться локально в зашифрованому вигляді на вашому комп’ютері, а не на сторонніх серверах, що зробить неможливим їхій витік. Якщо якимось чином база даних все-таки буде скомпроментована, усі ваші паролі все одно будуть захищені від несанкціонованого доступу, оскільки SecurePass використовує API захисту даних (DPAPI)[3] Windows, що забезпечує додатковий рівень безпеки завдяки шифруванн паролів за допомогою криптографічних ключів, які зберігаються на вашому комп’ютері. Це означає, що тільки ви можете розшифрувати свої паролі на своєму пристрої.

SecurePass включатиме в себе досить великий функціонал. Він буде мати вбудований генератор паролів, що дозволить користувачу генерувати сильні та унікальні паролі для кожного акаунту. Також буде доступний сканер паролів, який скануватиме усі паролі користувача на надійність, повторюваність та застарілість, допомагаючи користувачу покращити загальний рівень безпеки паролів та позбутися слабких ланок. Окрім цього, SecurePass матиме кошик для паролів, де зберігатимуться видалені паролі. Це надасть користувачу можливість відновити випадково видалені паролі. Також програма дозволятиме користувачу організовувати паролі за папками для кращої структури та зручності пошуку.

SecurePass пропонуватиме надзвичайно простий та інтуїтивно зрозумілий інтерфейс, що робитиме застосунок легким і доступним у налаштуванні та використанні для користувачів з будь-яким рівнем досвіду. Також додаток буде доступний українською та англійською мовами, що робитиме його зручним як для україномовних користувачів, так і для користувачів з різних країн.

SecurePass буде доступний безкоштовно, без будь-яких обмежень на функціонаьльність або термін використання.

Загалом, SecurePass пропонує ряд переваг, які роблять його привабливим вибором для користувачів, які шукають безпечний та зручний менеджер паролів з великим спектром функцій.

# РОЗДІЛ 2. ОСНОВНІ ТЕХНОЛОГІЇ РОЗРОБКИ SECUREPASS

Додаток SecurePass – це десктопний менеджер паролів, розроблений на мові програмування C# з використанням фреймворку WPF. Цей вибір мови та фреймворку забезпечує зручність розробки, високу продуктивність та гнучкість програми.

Основні технології, використані в SecurePass:

**Мова програмування C#:** C# – це потужна та універсальна мова програмування, яка широко використовується для розробки програмного забезпечення. Вона поєднує в собі високу продуктивність, зручність використання та широкий спектр можливостей. Можливості C# використовуються в SecurePass для реалізації логіки роботи програми, обробки даних та взаємодії з користувачем.

**Система обробки подій:** SecurePass використовує систему обробки подій для реагування на дії користувача, такі як натискання кнопок, введення даних, переміщення курсора та вибір пунктів меню. Це дозволяє програмі динамічно змінювати свій стан та виконувати відповідні дії.

**Фреймворк WPF:** Windows Presentation Foundation[4] – це фреймворк для розробки графічних інтерфейсів користувача (GUI) в .NET Framework. Він дозволяє створювати багаті та динамічні інтерфейси з використанням XAML розмітки та обробки подій. SecurePass використовує WPF для створення зручного та інтуїтивно зрозумілого інтерфейсу, який дозволяє користувачам легко додавати, редагувати та видаляти паролі.

**Розмітка XAML:** Extensible Application Markup Language[5] – це декларативна мова розмітки, яка використовується для опису структури та зовнішнього вигляду елементів GUI в WPF. Вона дозволяє чітко та лаконічно описувати структуру та зовнішній вигляд елементів інтерфейсу, роблячи код більш читабельним та зручним для модифікації.

**Log4net:**Log4net – це бібліотека журналювання для C#, яка використовується для запису інформації про роботу програми в журнальні файли. SecurePass використовує Log4net для реєстрації подій, помилок та іншої інформації, що допомагає в діагностиці проблем та аналізі роботи програми.

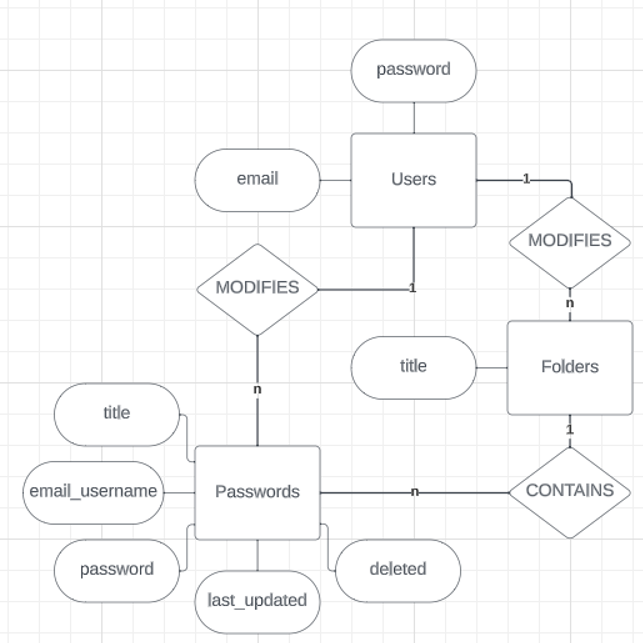
**StyleCop:** StyleCop – це інструмент статичного аналізу коду, який використовується для перевірки відповідності коду SecurePass стандартам програмування. Це допомагає покращити читабельність, узгодженість та загальну якість коду.

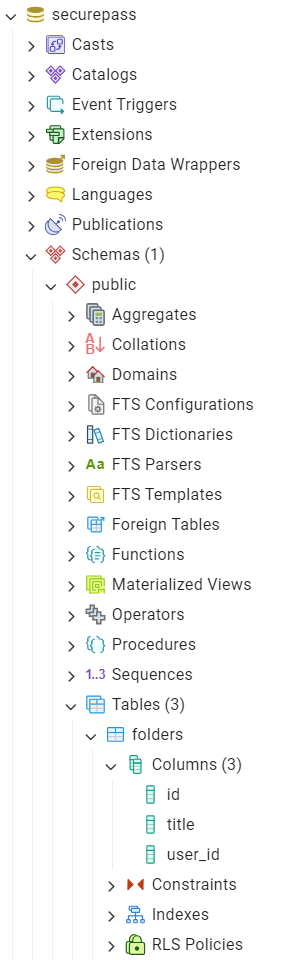
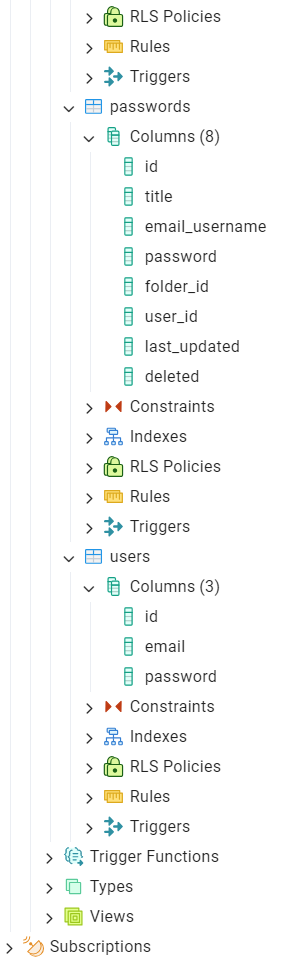
**DPAPI:** Data Protection Application Programming Interface – це стандарт Microsoft для шифрування даних, що забезпечує високий рівень безпеки та сумісність з операційними системами Windows. SecurePass використовує DPAPI для шифрування паролів в базі даних, щоб захистити їх від несанкціонованого доступу.

**Entity Framework Core:** Entity Framework Core[6] – це ORM (Object-Relational Mapping) фреймворк, який використовується для спрощення взаємодії з базою даних PostgreSQL. Він дозволяє розробникам працювати з даними на рівні об'єктів, не занурюючись у складні SQL-запити, роблячи код більш простим та зрозумілим.

**База даних PostgreSQL:** PostgreSQL[7] – це реляційна база даних з відкритим кодом, яка відома своєю надійністю, безпечністю та масштабованістю. SecurePass використовує PostgreSQL для зберігання паролів та інших даних користувачів.

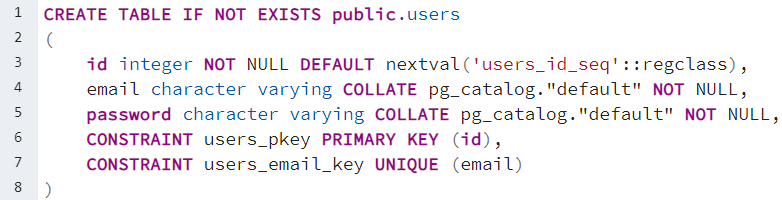
**Структура бази даних:**



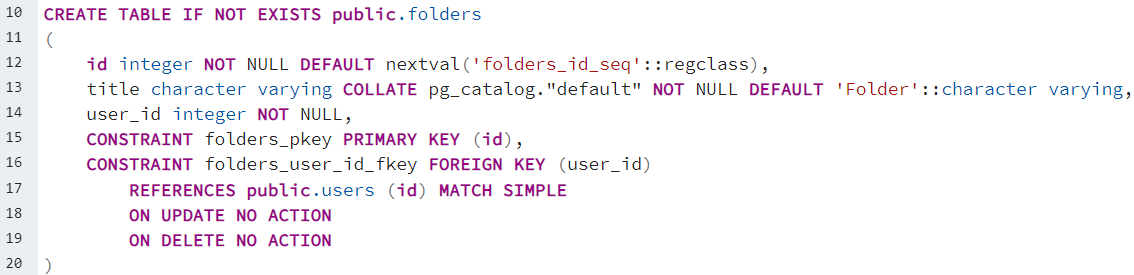
 

**SQL запити створення таблиць:**

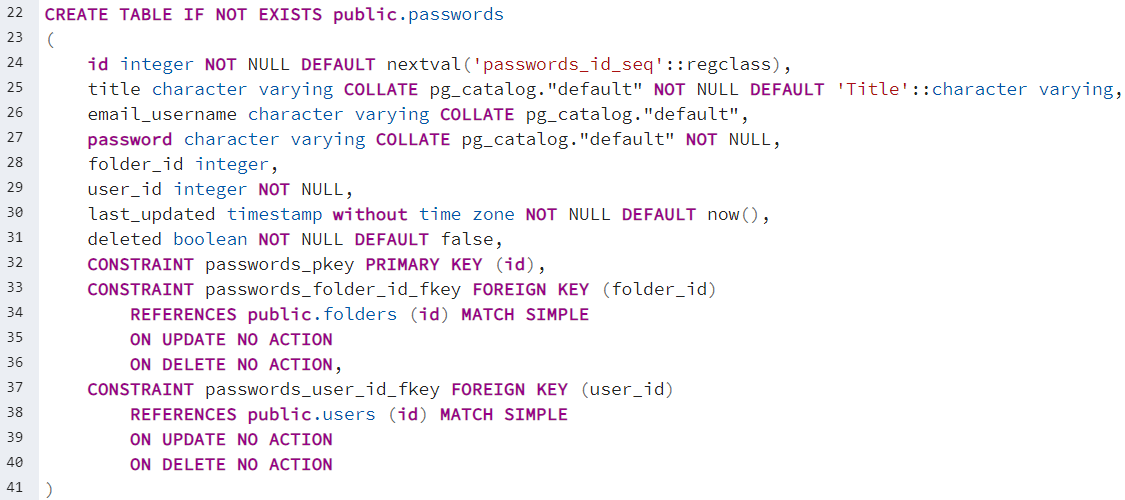
* **Таблиця Users:**
  + id: первинний ключ, ненульовий цілочисловий стовпець, для збереження унікального числового ідентифікатора для кожного користувача.
  + email: ненульовий стовпець типу “рядків змінної довжини”, для збереження адреси електронної пошти користувача.
  + password: ненульовий стовпець типу “рядків змінної довжини”, для збереження зашифрованого паролю користувача.



* **Таблиця Folders:**
  + id: первинний ключ, ненульовий цілочисловий стовпець, для збереження унікального числового ідентифікатора для кожної папки.
  + title: ненульовий стовпець типу “рядків змінної довжини”, для збереження назви папки.
  + user\_id: зовнішній ключ, ненульовий цілочисловий стовпець, для збереження ідентифікатору користувача.



* **Таблиця Passwords:**
  + id: первинний ключ, ненульовий цілочисловий стовпець, для збереження унікального числового ідентифікатора для кожного паролю.
  + title: ненульовий стовпець типу “рядків змінної довжини”, для збереження назви або мітки паролю.
  + email\_username: стовпець типу “рядків змінної довжини”, для збереження адреси електронної пошти або імені користувача, пов’язаних з паролем.
  + password: ненульовий стовпець типу “рядків змінної довжини”, для збереження зашифрованого паролю користувача.
  + folder\_id: зовнішній ключ, цілочисловий стовпець, для збереження ідентифікатору папки.
  + user\_id: ненульовий зовнішній ключ, цілочисловий стовпець, для збереження ідентифікатору користувача.
  + last\_updated: ненульовий стовпець, для збереження часового маркеру останнього оновлення запису про пароль.
  + deleted: ненульовий стовпець, для відмітки видалених паролів.



**Трирівнева архітектура:** застосунок SecurePass написаний з використанням трирівневої архітектури, яка розділяє програму на три чітко відокремлені рівні: рівень представлення (Presentation Layer), рівень бізнес-логіки (Business Logic Layer) та рівень доступу до даних (Data Access Layer).

Цей розподіл на рівні забезпечує ряд переваг:

* **Модульність:** Кожен рівень може розроблятися та тестуватися незалежно, що робить процес розробки більш гнучким та керованим.
* **Масштабованість:** Різні рівні можна масштабувати незалежно один від одного, що дозволяє легко адаптувати програму до зростаючих потреб.
* **Простота обслуговування:** Зміни на одному рівні не впливають на інші рівні, що робить обслуговування програми більш простим та ефективним.

Основні рівні архітектури:

* **Рівень представлення (Presentation Layer):** цей рівень відповідає за інтерфейс користувача (GUI) та взаємодію з користувачем. Основні функції рівня представлення включають в себе:
  + Відображення інтерфейсу користувача, включаючи вікна, панелі, кнопки, текстові поля та інші елементи.
  + Відображення та обробка даних, таких як списки паролів, інформацію про паролі та повідомлення про помилки.
  + Реагування на дії користувача, такі як натискання кнопок, введення даних та інші дії.
  + Забезпечення зв’язку з рівнем бізнес логіки для виконання різних операцій з паролями.

Рівень представлення не містить жодної бізнес-логіки програми. Він лише візуалізує дані та реагує на дії користувача, передаючи їх до рівня бізнес-логіки для їх подальшої обробки. У даному випадку, інтерфейс SecurePass знаходиться саме на цьому рівні. Він реалізований за допомогою фреймворку WPF та розмітки XAML.

* **Рівень логіки (Business Logic Layer):** цей рівень містить логіку роботи програми, яка відповідає за виконання основних функцій SecurePass, таких як:
  + Генерація, додавання, редагування, видалення, сканування, збереження, шифрування та дешифрування паролів користувача.
  + Автентифікація користувачів.
  + Створення, редагування та видалення папок користувача.

Рівень бізнес-логіки використовує різні класи та методи для реалізації цих функцій. Він взаємодіє з рівнем представлення для отримання даних від користувача та відображення результатів, а також з рівнем доступу до даних для роботи з базою даних. Основний функціонал програми знаходиться саме на цьому рівні. Він реалізований за допомогою мови програмування C#.

* **Рівень доступу до даних (Data Access Layer):** цей рівень відповідає за доступ до даних, які використовуються програмою. Основні функції рівня доступу до даних:
  + Підключення до бази даних PostgreSQL.
  + Виконання CRUD-операцій (Create, Read, Update, Delete) з даними.
  + Забезпечення цілісності та узгодженості даних.

Рівень доступу до даних не залежить від логіки роботи програми і використовується лише для доступу до даних та їх менеджменту. У даному випадку, рівень доступу до даних реалізований за допомогою набору технологій ADO.NET, а сама база даних реалізована за допомогою PostgreSQl.

A screenshot of a computer program

Description automatically generated A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated A screenshot of a computer screen

Description automatically generated

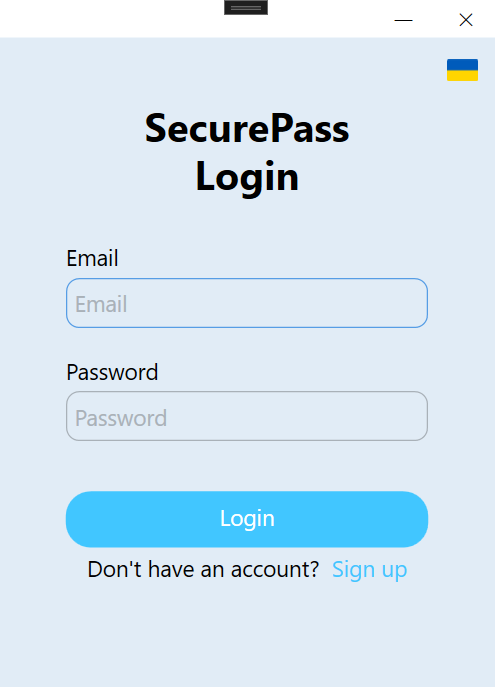
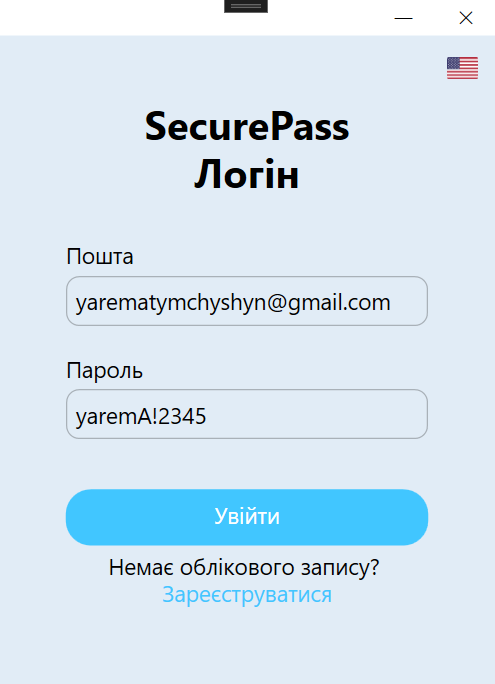
Використання всіх вище перелічених технологій дозволило створити надійний, зручний та багатофункціональний менеджер паролів SecurePass. Всі ці методи та функції посприяли ефективній розробці та підтримці застосунку, надаючи SecurePass зручний та інтуїтивно зрозумілий інтерфейс користувача, надійну логіку обробки даних, безпечний доступ до даних та високий рівень безпеки їхнього зберігання.

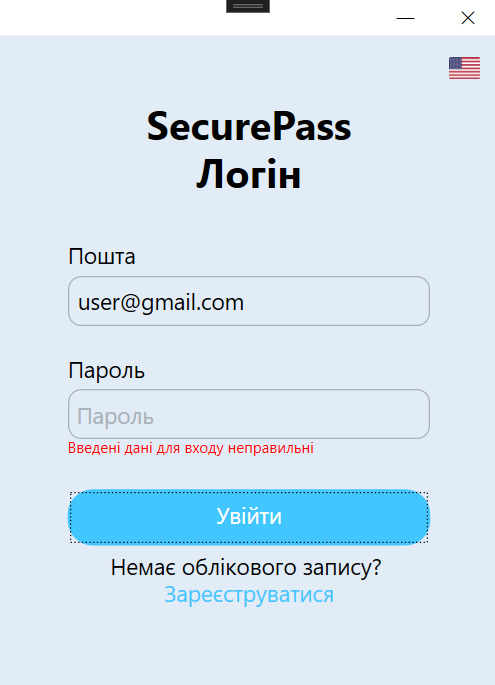
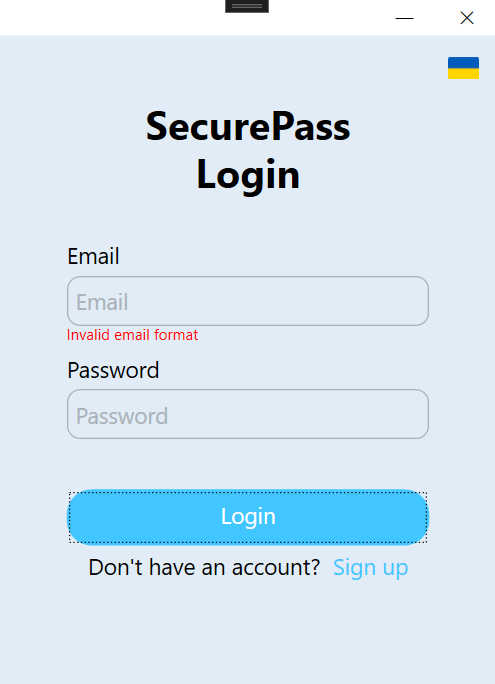
# РОЗДІЛ 3. ІНТЕРФЕЙС ТА ОСНОВНА РОБОТА ПРОГРАМИ

SecurePass має простий та інтуїтивно зрозумілий інтерфейс, що дозволяє легко користуватися застосунком і без зайвих проблем знаходити необхідні користувачу кнопки. Програма складається з трьох вікон та восьми сторінок, що забезпечує користувача всім необхідним для менеджменту паролів. Далі детально описується кожен з елементів інтерфейсу.

**Вікно логінації:**

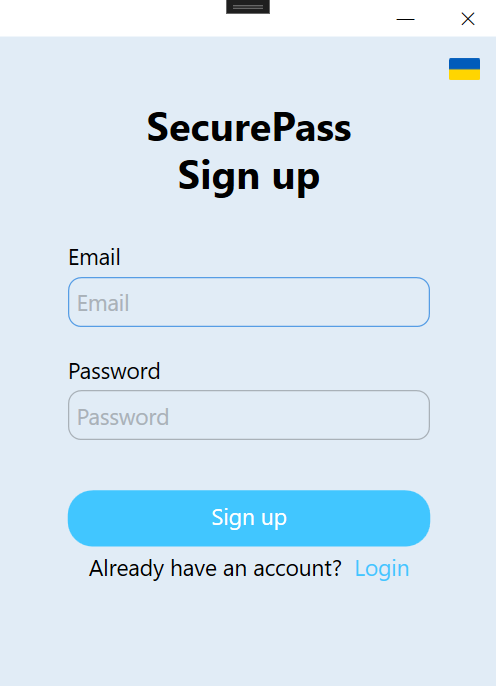
Вікно логінації складається з текстового поля для введення електронної пошти користувача, текстового поля для введення паролю користувача, клікабельної іконки для зміни мови інтерфейсу програми, кнопки для входу, та посилання на вікно реєстрації. На текстових полях для введення пошти та паролю стоїть валідація даних, яка перевіряє чи взагалі якісь дані були введені, чи правильний формат пошти (example@mail.com) та чи введений пароль правильний (відповідає пошті користувача). Якщо ж введена інформація не відповідає вимогам, то з’являється текст-пояснення помилки.

**Вікно реєстрації:**

Вікно логінації складається з текстового поля для введення електронної пошти користувача, текстового поля для введення паролю користувача, клікабельної іконки для зміни мови інтерфейсу програми, кнопки для реєстрації та посилання на вікно логінації. На текстових полях для введення пошти та паролю стоїть валідація даних, яка перевіряє чи взагалі якісь дані були введені та чи правильний формат пошти (example@mail.com). Якщо введена інформація не відповідає вимогам, то з’являється текст-пояснення помилки.



**Сторінка паролів:**

Ця сторінка складається по суті із двох рамок.

Рамка зліва містить в собі іконку користувача, при натисканні якої з’являється випадаюче вікно, що пропонує вийти з акаунту поточного користувача; іконку налаштувань, при натискавнні якої з’являється випадаюче вікно, що пропонує опцію зміни мови інтерфейсу; ярлики для навігації між сторінками паролів, папок, смітника та сканера паролів.

Тоді як рамка справа містить в собі кнопку додавання паролю, при натисканні якої відкриється сторінка створення паролю та список усіх паролів користувача. Кожен запис паролю складається з назви, під назвою може бути вказана пошта або логін, пов’язаний з паролем, далі відображений сам пароль, який по замовчуванню прихований, і далі, якщо навести на пароль курсором, з’являються чотири кнопки, перша з яких показує уже неприхований пароль, друга копіює пароль, третя відкриває сторінку створення паролю, де можна відредагувати пароль, а четверта – переносить пароль в кошик. У випадку коли паролів дуже багато, справа збоку додатково з’являється слайдер.

A screenshot of a computer

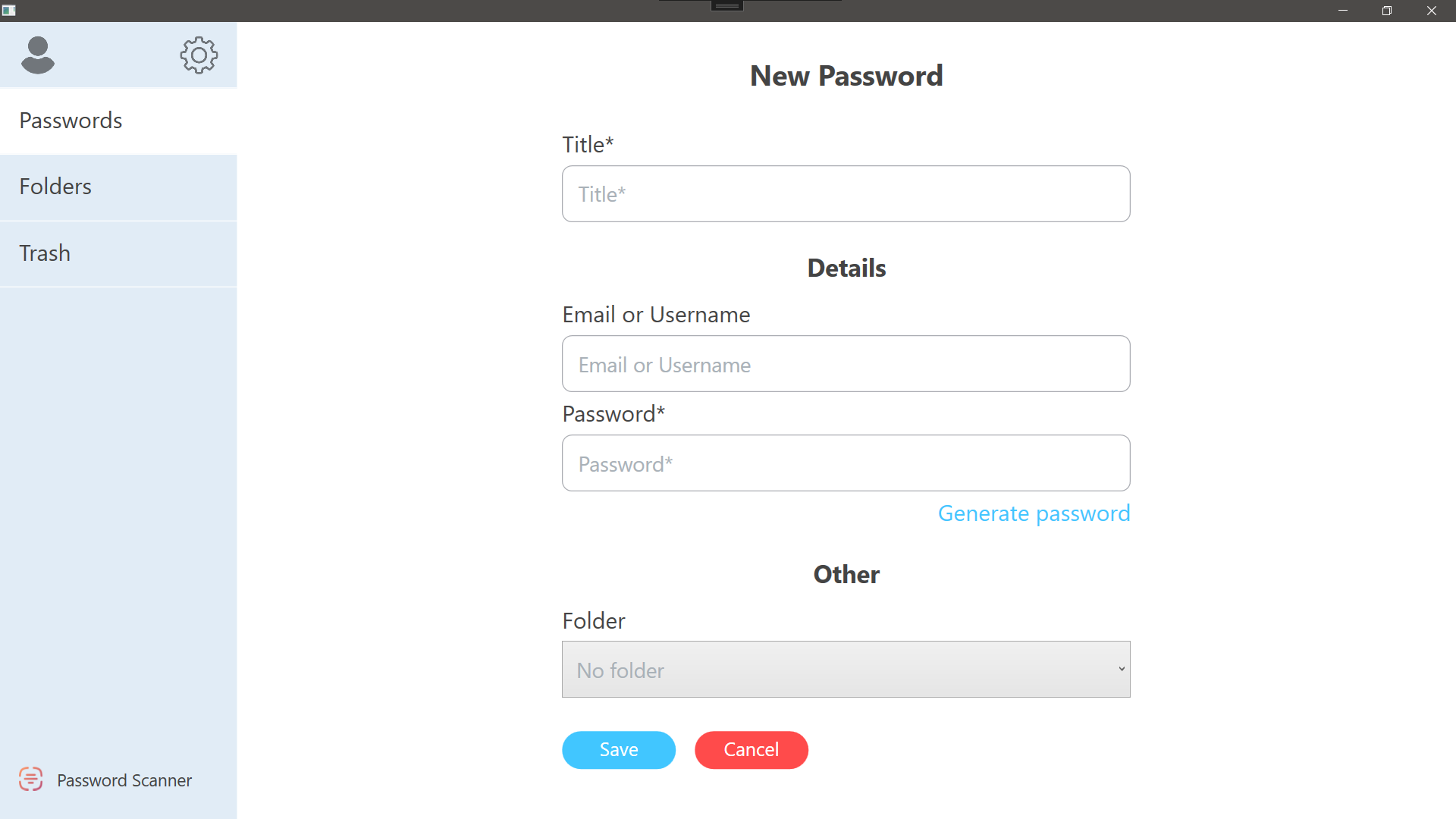
Description automatically generated

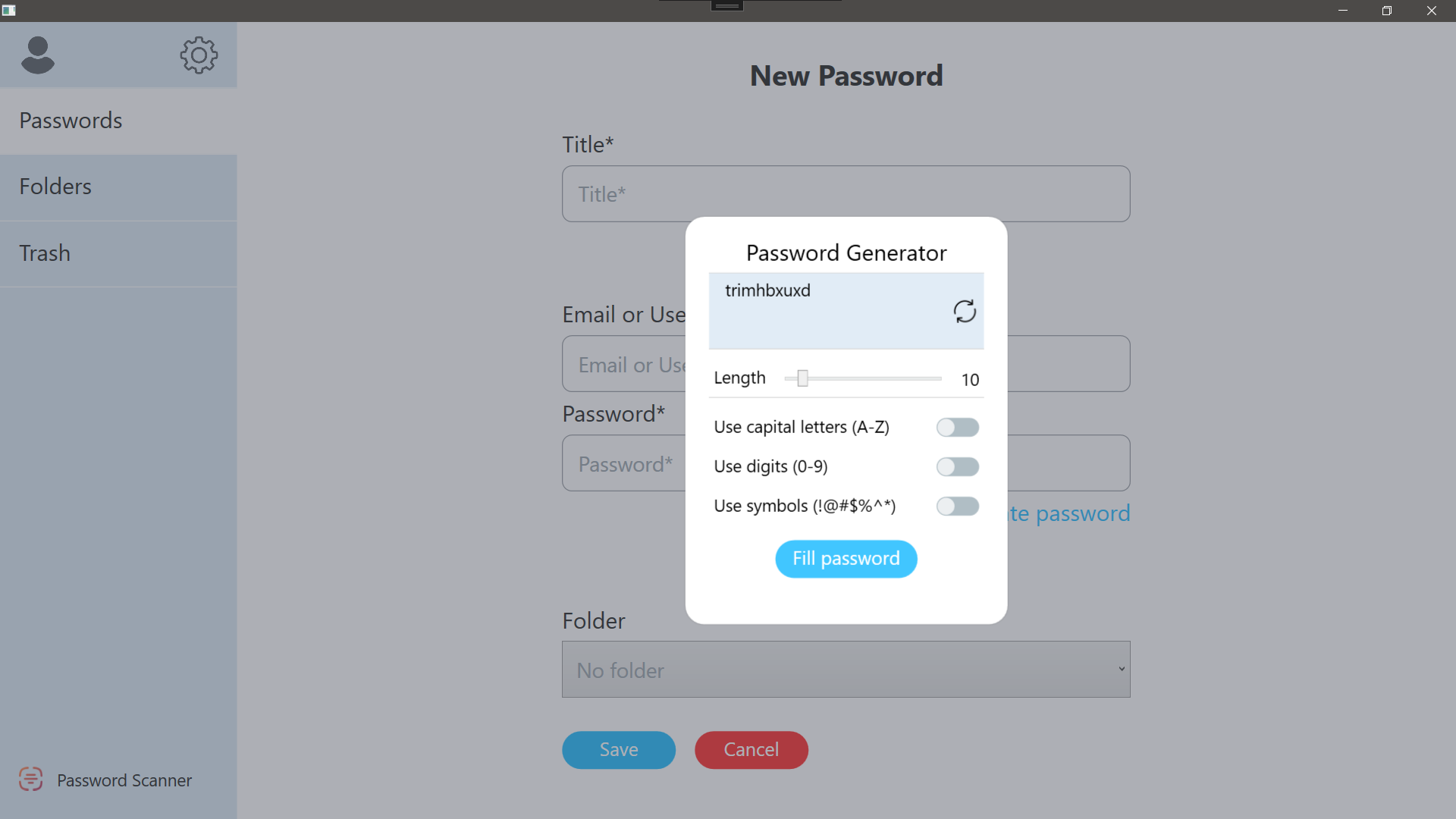
**Сторінка створення паролю:**

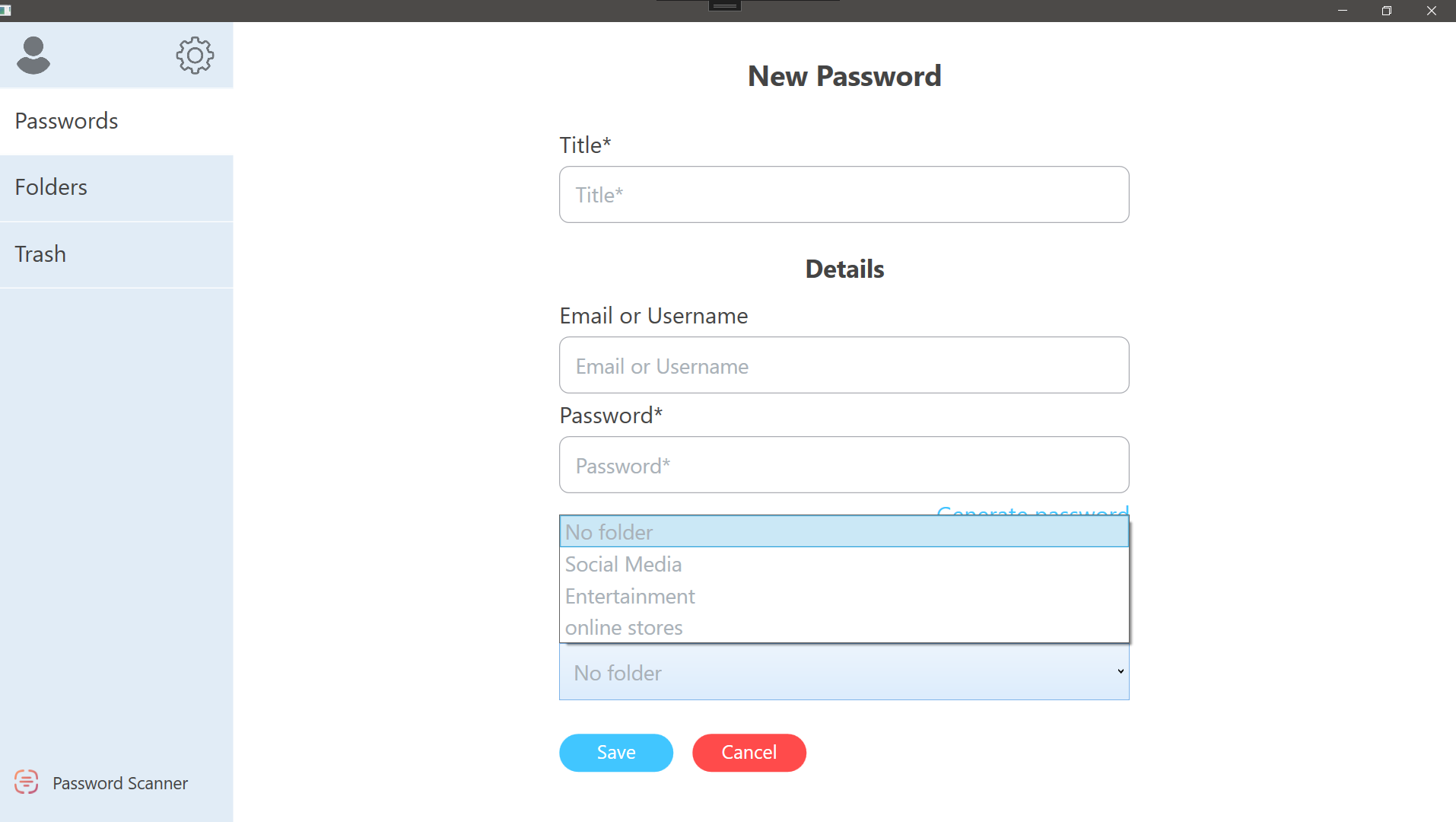
Ця сторінка теж складається із двох рамок. Рамка зліва аналогічна як на попередній сторінці.

Рамка справа містить три текстові поля, випадаючий список, де можна вибрати в яку папку зберегти пароль, кнопку, при натисканні з’являється вікно генератора паролів, та кнопок для підтвердження або скасування додавання паролю. На текстових полях пристуня валідація, тому що поле “Title” та поле “Password” обов’язково повинні бути заповненими. Якщо спробувати зберегти пароль з незаповненими цими полями, то з’являється текст-пояснення помилки.

Вікно генератора паролів складається із полотна на якому знаходиться пароль і кнопка для перегенерації паролю; повзунка, за допомогою можна вибрати довжину паролю (від 5 до 50 символів); трьох важелів, за допомогою яких можна використовувати або не використовувати великі літери, цифри та спеціальні символи в генерації паролю; та кнопки підтвердження паролю.



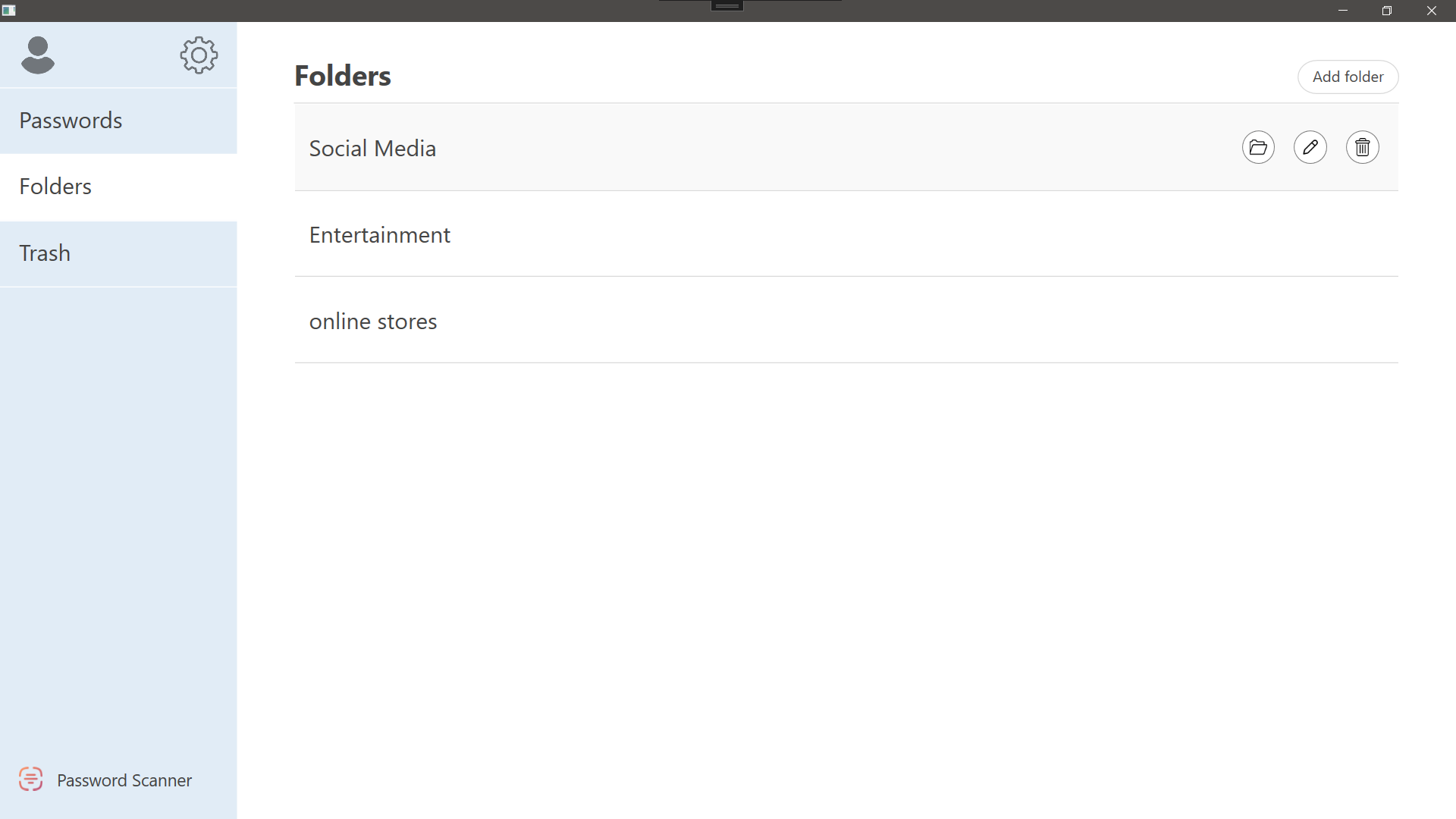




**Сторінка папок:**

Ця сторінка теж складається із двох рамок. Рамка зліва аналогічна як на попередній сторінці.

Рамка справа містить в собі кнопку додавання папки, при натисканні якої відкриється вікно створення папки, яке складається з текстового поля для введення назви папки та кнопки підтвердження створення нової папки; та список усіх папок користувача. Кожен запис папки складається лише з назви, проте якщо навести на папку курсором, то з’явиться три кнопки, перша з яких відкриває папку, друга відкриває вікно створення папки, де можна відредагувати назву папки, і третя кнопка, яка видаляє папку.



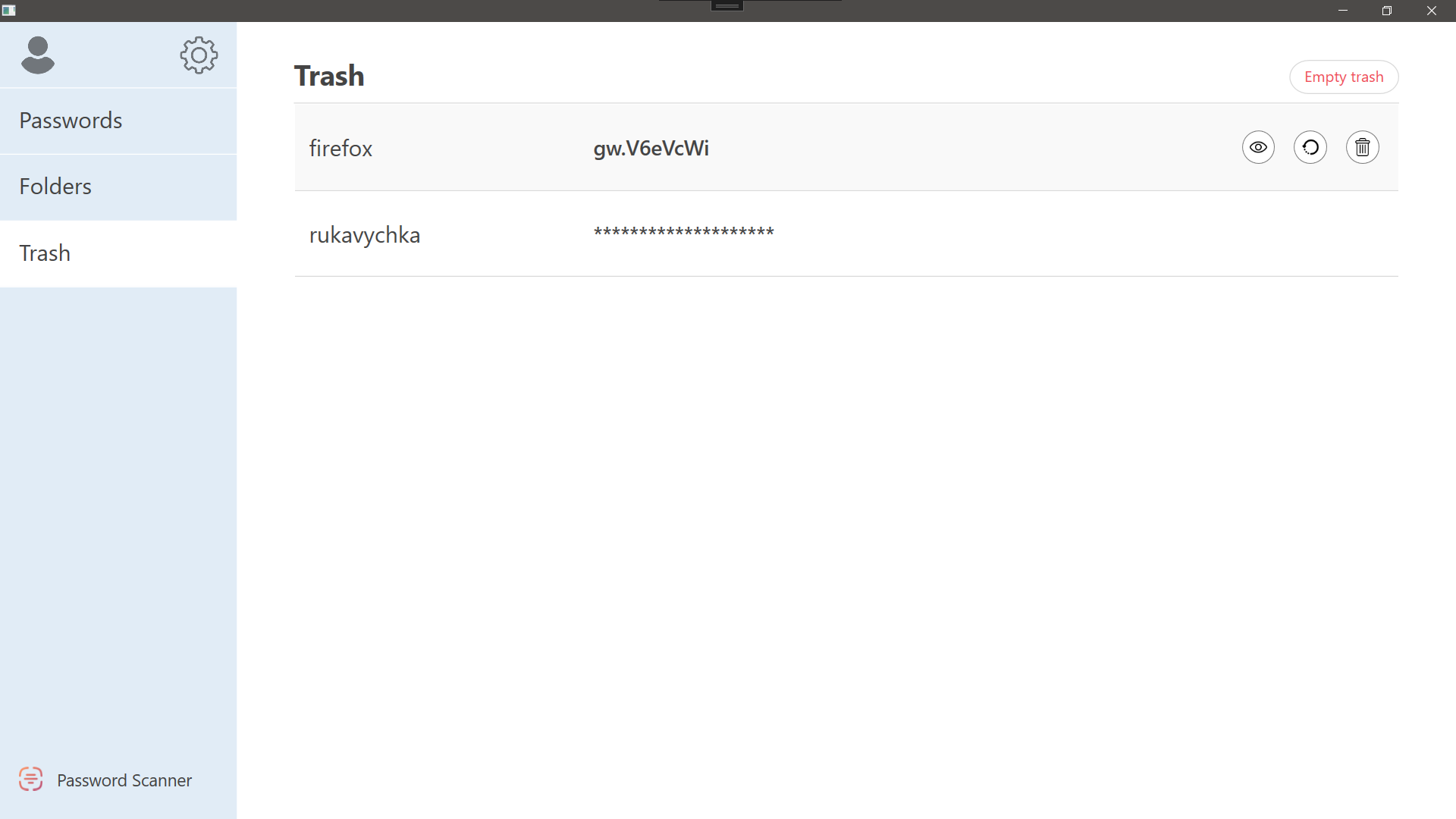
A screenshot of a computer

Description automatically generated

**Сторінка смітника:**

Ця сторінка теж складається із двох рамок. Рамка зліва аналогічна як на попередній сторінці.

Рамка справа містить в собі кнопку очищення смітника, при натисканні якої всі паролі перманентно видаляються; та списку всіх паролів, що були перенесені в кошик. Кожен запис паролю складається з назви, під назвою може бути вказана пошта або логін, пов’язаний з паролем, далі відображений сам пароль, який по замовчуванню прихований, і далі, якщо навести на пароль курсором, з’являються три кнопки, перша з яких показує уже неприхований пароль, друга відновлює пароль, а третя перманентно видаляє пароль.



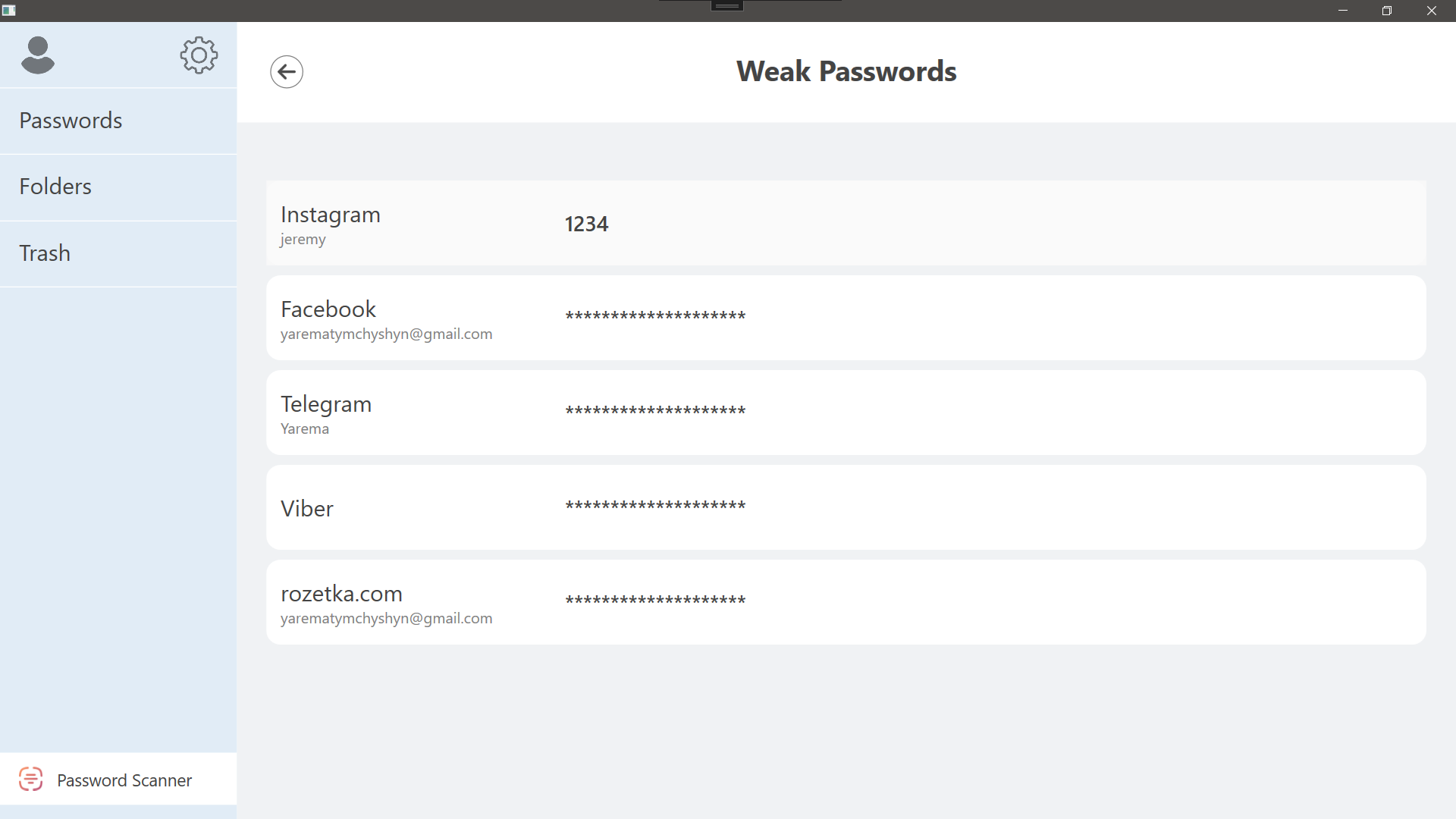
**Сторінка сканера паролів:**

Ця сторінка теж складається із двох рамок. Рамка зліва аналогічна як на попередній сторінці.

Рамка справа містить в собі ще три рамки. Перша рамка показує кількість ненадійних паролів; друга рамка показує кількість повторюваних паролів; третя рамка показує кількість застарілих паролів. При натискані на кожну з них, відкриються відповідні сторінки, з переліком цих паролів. Кожен запис паролю складається з назви, під назвою може бути вказана пошта або логін, пов’язаний з паролем, далі відображений сам пароль, який по замовчуванню прихований, і далі, якщо навести на пароль курсором, з’являються дві кнопки, перша з яких показує уже неприхований пароль, а друга відкриває сторінку створення паролю, де можна відредагувати пароль.

A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

# ВИСНОВКИ

Застосунок “SecurePass” є корисним інструментом для управління паролями та підвищення безпеки в мережі. Реалізована функціональність застосунку включає зберігання, генерування та надійне зберігання, що дозволяє користувачам ефективно та безпечно керувати своїми обліковими даними.

Менеджер паролів "SecurePass" є зручним і надійним інструментом для користувачів. Він дозволяє зберігати та організовувати паролі в одному безпечному місці, що зменшує ризик їх втрати або викрадення. Застосунок може бути корисним для підготовки до роботи в умовах підвищеної кібербезпеки та допомагати користувачам підвищити захист своїх персональних даних.

Розробка застосунку "SecurePass" для ефективного управління паролями є актуальним завданням. Дослідження в цій області включає аналіз сучасних методів шифрування та стандартів безпеки.

Не менш важливо є і те, що потенціал для подальшого розвитку застосунку є надзвичайно великим, зокрема включення функцій двофакторної аутентифікації та підтримки біометричних даних. Це дозволить користувачам ще більше підвищити рівень безпеки своїх облікових записів та забезпечить їм комплексний захист у мережі. Для вдосконалення застосунку можна використовувати сучасні методи шифрування та інші інноваційні технології.

Розробка нового вмісту, пов'язаного з додатковими функціями безпеки, є ключовим етапом для забезпечення повного захисту облікових даних за допомогою застосунку. Це включає використання сучасних алгоритмів шифрування та методів аутентифікації.

Узагальнюючи, застосунок "SecurePass" є корисним інструментом для управління паролями та підвищення безпеки в мережі, а його подальше вдосконалення з урахуванням новітніх технологій може розширити його функціональність та дозволити користувачам отримати комплексний захист своїх даних через інтерактивну взаємодію з додатком.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. [Який обсяг пам'яті має людський мозок?](https://www.cnsnevada.com/what-is-the-memory-capacity-of-a-human-brain/)
2. [Цей чоловік володіє 321 мільйоном доларів у біткоїнах, але не може отримати до них доступ, бо втратив пароль](https://www.cbc.ca/radio/asithappens/as-it-happens-friday-edition-1.5875363/this-man-owns-321m-in-bitcoin-but-he-can-t-access-it-because-he-lost-his-password-1.5875366)
3. [How to use data protection](https://learn.microsoft.com/en-us/dotnet/standard/security/how-to-use-data-protection)
4. [Windows Presentation Foundation documentation](https://learn.microsoft.com/en-us/dotnet/desktop/wpf/?view=netdesktop-8.0)
5. [XAML Services](https://learn.microsoft.com/en-us/dotnet/desktop/xaml-services/?redirectedfrom=MSDN)
6. [Entity Framework Core](https://learn.microsoft.com/en-us/ef/core/)
7. [PostgreSQL 16.3 Documentation](https://www.postgresql.org/docs/current/)
8. Hejlsberg, A., Torgersen, M., Wiltamuth, S., & Golde, P. (2010). The C# Programming Language (4th ed.).