**МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ АТОМНОЇ ТА ТЕПЛОВОЇ ЕНЕРГЕТИКИ**

**КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ЕНЕРГЕТИЦІ**

ПУНКТИ 1-4 КУРСОВОЇ РОБОТИ

**з дисципліни:** ««Основи Веб-програмування»

**на тему:** «Додаток, який створює сильні та безпечні паролі»

**Виконав**:

Семенов Максим Михайлович

Студент 2 курсу

Групи ТВ-32

Посилання на **GitHub** репозиторій: <https://github.com/max-s-m/web-kursova1-4>

**Київ - 2025**

**Розділ 1. Створення діаграм компонентів, взаємодії та класів веб-додатку.**

A black screen with white ovals

AI-generated content may be incorrect.

Рисунок 1.1 - Діаграма варіантів використання

A screenshot of a computer

AI-generated content may be incorrect.

Рисунок 1.2 – Діаграма послідовності генерації паролю

A diagram of a company

AI-generated content may be incorrect.

Рисунок 1.3 – Діаграма компонентів

1. Користувачеві буде можливий доступ до сховища паролів:
   1. Екран для введення майстер-ключа:
      1. При першому використанні з новим ключем – створення сховища.
      2. При наступних – розшифрування даних для доступу.
   2. Перевірка коректності майстер-ключа через розшифрування спеціального маркера.
   3. Відображення повідомлень про помилку введення ключа або статус операції.
   4. Функція блокування сховища (вимагає повторного введення ключа).
2. Користувач зможе генерувати паролі, для чого буде реалізовано:
   1. Форма налаштування параметрів генерації:
      1. Введення довжини пароля.
      2. Введення кількості символів латиниці, кирилиці, спеціальних символів.
      3. Введення списку дозволених спеціальних символів.
      4. Автоматичне додавання цифрових символів для досягнення заданої довжини.
   2. Алгоритм генерації пароля на основі введених параметрів.
   3. Відображення згенерованого пароля.
3. Можна буде редагувати записи паролів:
   1. Додавання нового запису (логін + пароль):
      1. Форма для введення власного логіна та пароля.
      2. Форма для введення логіна та збереження раніше згенерованого пароля.
      3. Шифрування логіна та пароля на стороні клієнта майстер-ключем перед збереженням.
   2. Перегляд збережених паролів:
      1. Відображення списку пар логін/пароль після введення майстер-ключа.
      2. Розшифрування даних на стороні клієнта перед відображенням.
   3. Видалення запису пароля:
      1. Можливість видалення запису за введеним логіном.
      2. Шифрування введеного логіна майстер-ключем для пошуку відповідного запису.
   4. Відображення повідомлень про статус операцій (додавання, видалення).
4. Частиною функціоналу буде зберігання та шифрування даних:
   1. Шифрування/дешифрування логінів та паролів на стороні клієнта за допомогою майстер-ключа. Майстер-ключ не передається на сервер у відкритому вигляді.
   2. Алгоритм шифрування на основі динамічної мапи заміни символів, залежної від майстер-ключа.
   3. Зберігання зашифрованих версій логінів та паролів у базі даних MySQL.
   4. Зберігання на сервері спеціального маркера, зашифрованого майстер-ключем, для валідації ключа.
5. Користувач матиме простий інтерфейс, який включатиме:
   1. Поділ функціоналу на екрани: введення ключа, головне меню, перегляд, редагування, генерація.
   2. Візуальне оформлення з можливістю встановлення фонового зображення та відображенням логотипу.
   3. Адаптивність інтерфейсу для різних розмірів екранів.

**Розділ 2. Проектування структури меню з урахуванням потреб користувача**

Основна взаємодія користувача з програмою "Генератор Паролів" відбувається через послідовність екранів та меню, що відображаються залежно від поточного стану програми (наприклад, чи введено майстер-ключ) та обраних дій.

Після успішного введення майстер-ключа, користувачу буде доступне Головне Меню, яке включатиме наступні пункти:

* Переглянути паролі
* Додати/видалити пароль
* Заблокувати сховище (Вихід)

A diagram of a circle and a circle

AI-generated content may be incorrect.

Рисунок 2.1 - Схематичне зображення головного меню програми

Опис пунктів Головного Меню та пов'язаних з ними екранів/дій:

1. Переглянути паролі:
   1. Цей пункт меню переведе користувача на екран відображення списку збережених логінів та паролів.
   2. Дані будуть розшифровані поточним майстер-ключем та представлені у зручному для читання форматі.
   3. З цього екрану буде доступна кнопка для повернення до головного меню.
2. Додати/видалити пароль:
   1. Цей пункт меню переведе користувача на екран "Редагування паролів", який є підменю з наступними опціями:
      1. Додати пароль (переводить на екран "Додавання паролю", де користувач може обрати додавання або генерування паролю).

A screenshot of a phone

AI-generated content may be incorrect.

Рисунок 2.2 – Схематичне зображення меню генерації

* + 1. Видалити пароль (переводить на екран "Видалення паролю", де користувачеві буде запропоновано ввести логін/ресурс, запис якого необхідно видалити.
    2. Повернутися до Головного Меню: Закриває екран "Редагування паролів" та повертає користувача до Головного Меню.

1. Заблокувати сховище (Вихід)
   1. Цей пункт меню здійснює вихід з поточного сеансу роботи зі сховищем.
   2. Майстер-ключ скидається, і для подальшого доступу до даних його потрібно буде ввести знову (користувач перенаправляється на екран введення майстер-ключа).

**Розділ 3. Розміщення та стилізація елементів інтерфейсу**

Інтерфейс програми "Генератор Паролів" складається з кількох екранів:

1. Екран введення Майстер-ключа:
   1. На екрані присутні:  
      - Поле для введення майстер-ключа.  
      - Кнопка "Розблокувати / Створити сховище".  
      - Область для відображення повідомлень (про помилку або успіх).

A screenshot of a computer screen

AI-generated content may be incorrect.

Рисунок 3.1 - Схема розміщення елементів інтерфейсу екрана введення майстер-ключа

1. Головне Меню (після розблокування):
   1. На екрані вертикально розміщені кнопки:  
      - "Переглянути паролі".  
      - "Додати/видалити пароль".  
      - "Заблокувати сховище (Вихід)".
2. Екран "Редагування паролів":
   1. На екрані вертикально розміщені кнопки:  
      - "Додати пароль".  
      - "Видалити пароль".  
      - "Повернутися до Головного Меню".
3. Екран "Додавання паролю":
   1. Кнопки вибору режиму:  
      - "Ввести свій пароль".  
      - "Згенерувати пароль".
   2. При виборі "Ввести свій пароль":  
      - Поле для введення логіна/ресурсу.  
      - Поле для введення пароля.  
      - Кнопка "Зберегти".
   3. При виборі "Згенерувати пароль":  
      - Поля для параметрів генерації (довжина, типи символів).  
      - Кнопка "Згенерувати".  
      - Область відображення згенерованого пароля.  
      - Поле для введення логіна/ресурсу (для згенерованого пароля).  
      - Кнопка "Зберегти згенерований пароль".
   4. Кнопка "Назад до Редагування".
   5. Область для повідомлень.

A screenshot of a phone

AI-generated content may be incorrect.

Рисунок 3.2 - Схема розміщення елементів інтерфейсу екрана додавання паролю

1. Екран "Видалення паролю":
   1. На екрані присутні:  
      - Поле для введення логіна/ресурсу для видалення.  
      - Кнопка "Видалити".  
      - Кнопка "Назад до Редагування".  
      - Область для повідомлень.
2. Екран "Список Паролів":
   1. Область для динамічного відображення списку розшифрованих пар логін/пароль.
   2. Кнопка "Назад до Головного Меню".

Загальні елементи стилізації:

* Використання фонового зображення для всієї сторінки.
* Відображення логотипу над основним робочим вікном програми.
* Центральне розміщення основного вікна та його елементів.
* Кнопки та поля вводу стилізовані для чіткості та зручності.

**Розділ 4. Проектування моделей даних для збереження інформації**

В системі передбачено наступні основні сутності даних для зберігання інформації в базі даних MySQL:

* Запис Пароля (Password Entry)
* Маркер Валідації (Validation Marker)

A black background with a black square

AI-generated content may be incorrect.

Рисунок 4 - Діаграма моделей даних для збереження інформації

Модель даних "Запис Пароля" зберігає інформацію про кожен окремий логін та пов'язаний з ним пароль у зашифрованому вигляді.

Атрибути:

* id (первинний ключ, автоінкремент)
* encrypted\_login (зашифрований логін/ресурс)
* encrypted\_password (зашифрований пароль)

Модель даних "Маркер Валідації" зберігає спеціальний зашифрований рядок, який використовується для перевірки коректності майстер-ключа без необхідності дешифрування всіх записів паролів.

Атрибути:

* id (первинний ключ, автоінкремент)
* marker\_key (унікальний текстовий ідентифікатор маркера)
* encrypted\_value (зашифроване значення маркера)