УДК 004.056.53

ПРОГРАМНИЙ СЕРВІС ДЛЯ АВТОМАТИЧНОЇ ПЕРЕВІРКИ ПАРАМЕТРІВ БЕЗПЕКИ ПЕРСОНАЛЬНИХ СТОРІНОК КОРИСТУВАЧІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

Шевчук Р.П.[1)], Опалько О.О.[2)]
Тернопільський національний економічний університет
[1)]к.т.н., доцент, [2)]магістрант

Вступ

Сьогодні переважна більшість користувачів Інтернет недооцінюють ризики інформаційної безпеки в соціальних мережах. Незважаючи на удосконалення технологій в області захисту інформації, вразливість персональних сторінок користувачів у соціальних мережах продовжує зростати. Підтвердженням цього факту є масові повідомлення про злами та витік даних із облікових записів користувачів соціальних мереж [1-4]. Як правило, причиною цих інцидентів є незнання користувачами наявних параметрів безпеки облікових записів, які реалізовані розробниками соціальних мереж та рекомендуються фахівцями із інформаційної безпеки [5].

II. Постановка задачі

Безпека персональних сторінок користувачів соціальних мереж є взаємозв'язаною сукупністю засобів контролю безпеки, які реалізовані на стороні сервера соціальної мережі та ряду додаткових параметрів, які необхідно періодично перевіряти/налаштовувати користувачу [5].

У роботах [5,6] виділено параметри безпеки персональних сторінок користувачів реалізовані на стороні сервера у соціальних мережах Facebook, YouTube, Instagram, а також параметри безпеки, реалізовані на зовнішніх інтернет – сервісах, які дозволяють комплексно налаштувати безпеку персональних сторінок користувачів. Такими параметрами є: двоетапна перевірка; приватний обліковий запис; сповіщення про безпеку та конфіденційність; перевірка авторизованих входів; формування довірених контактів; генерування кодів ідентифікації; перевірка складності пароля; перевірка витоків пароля; перевірка витоків даних для адреси електронної скриньки; регулярна зміна пароля; перевірка доступу зовнішніх застосунків до облікового запису [5]. Як правило, більшість користувачів соціальних мереж слабо обізнані із особливостями налаштування параметрів безпеки у соціальних мережах, що призводить до збільшення ризиків зламу сторінки чи витоку конфіденційних даних.

Тому постає задача створення програмного сервісу для автоматичної перевірки параметрів безпеки персональних сторінок користувачів у соціальних мережах.

III. Мета роботи

Метою роботи є розробка програмного сервісу для автоматичної перевірки параметрів безпеки персональних сторінок користувачів у соціальних мережах, який дозволить сформувати рекомендації щодо підвищення рівня їх захищеності.

IV. Особливості розробки програмного сервісу

Для реалізації програмного сервісу використано середовище розробки Visual Studio Professional 2019, API-функції сервісу Have I Been Pwned [7], а також API-функції соціальних мереж Facebook та Instagram [8]. На рисунку 1 подано архітектуру програмного сервісу, яка складається із трьох рівнів:

- User Interface – графічний інтерфейс користувача;
- Domain Logic – рівень, на якому реалізовано структурну та алгоритмічну складову програмного сервісу. Модуль Business Logic Services відповідає за логіку виконання запитів до бази даних. Модуль Process Centric Services відповідає за логіку виконання запитів до модулів Business Logic Services та Storage Service.
- Datasourses – рівень даних, представлений у вигляді баз даних та модулів, що з ними взаємодіють. Модуль Storage Services відповідає за аналіз та запис даних із персональної сторінки користувача у базу даних Postgres Server. Local Database Services - локальні служби баз даних, за допомогою яких відбувається аналіз вхідних даних у Storage Services і в подальшому проводиться їх запис у базу даних. Модуль Adapter Services отримує та конвертує дані із серверів на яких реалізовано API-функцій соціальних мереж (Facebook API, Instagram API) та API функцій сервісу Have I Been Pwned.

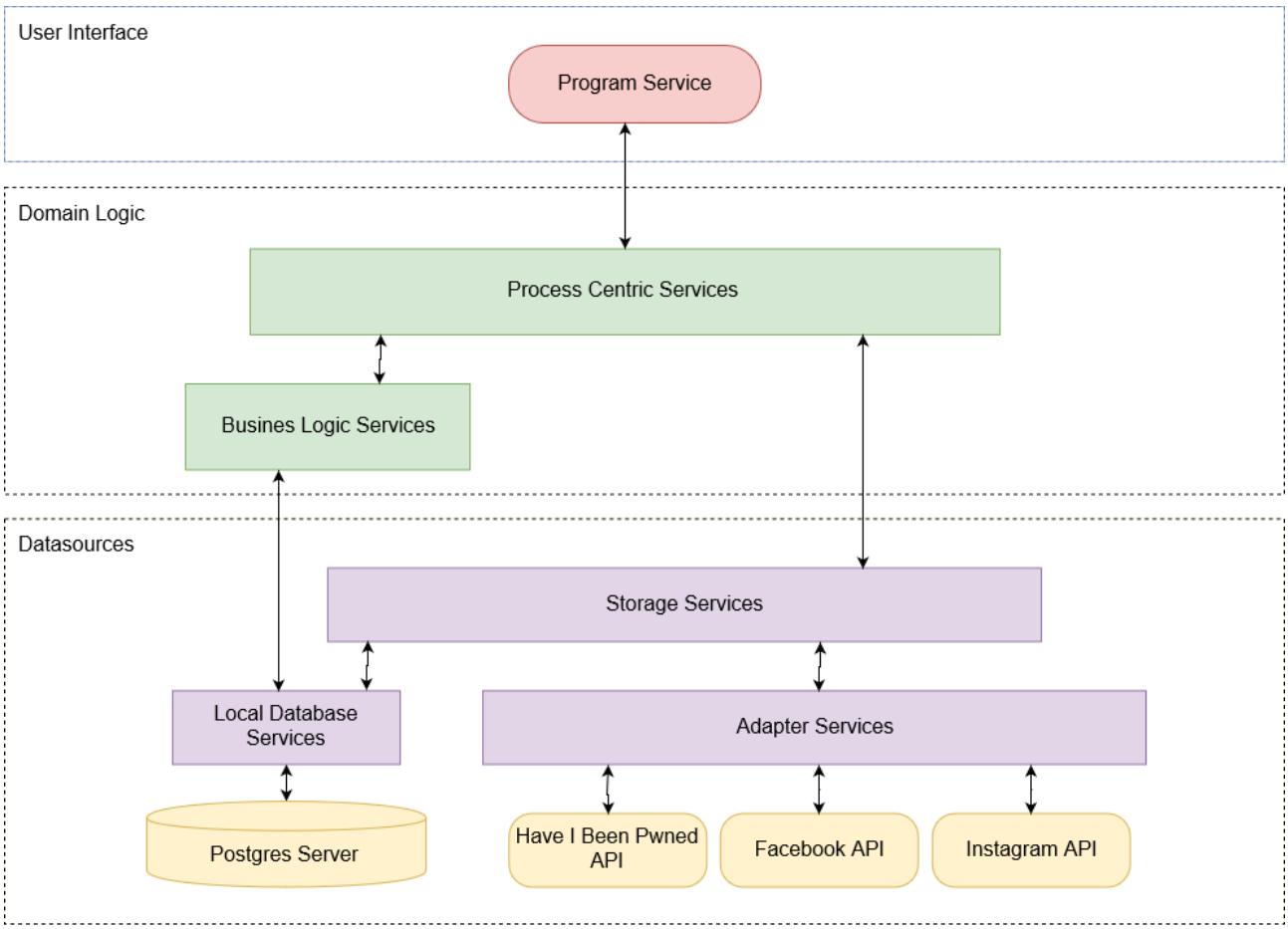

Рисунок 1- Архітектура програмного сервісу

На рисунку 2 подано діаграму варіантів використання програмного сервісу.

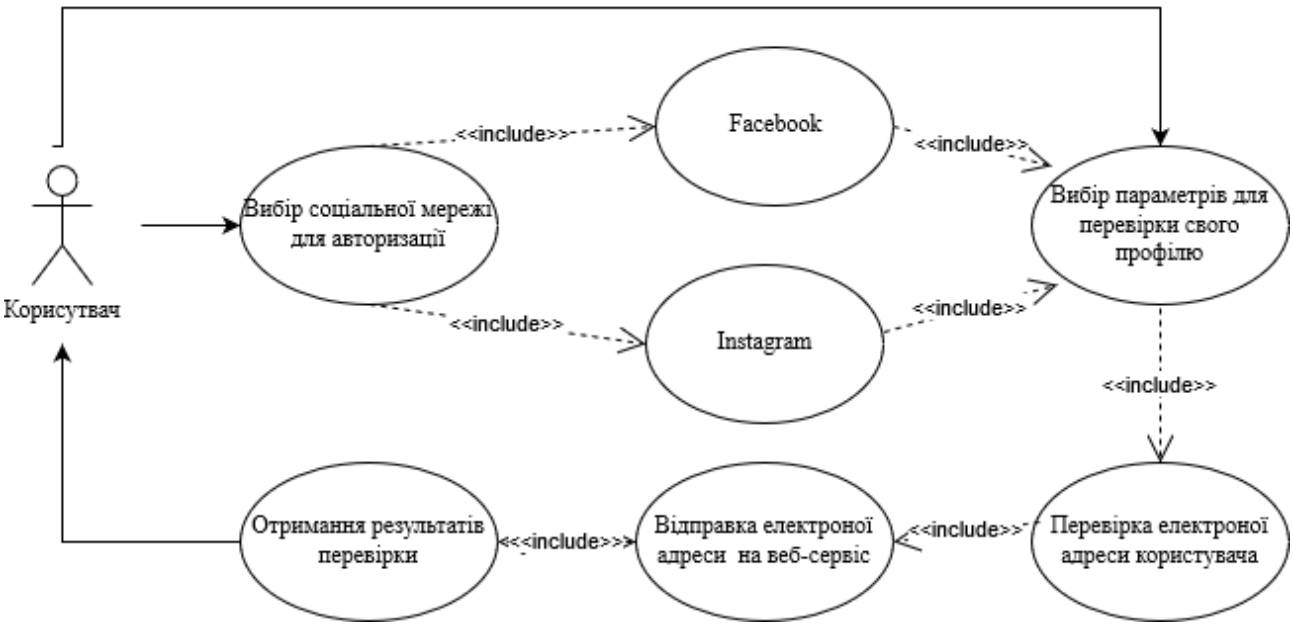

Рисунок 2 – Діаграма варіантів використання

Для роботи з програмним сервісом користувач повинен ідентифікуватись у соціальній мережі та натиснути кнопку «Check security» (рисунок 3). Після перевірки параметрів безпеки користувач отримає звіт щодо параметрів безпеки налаштованих для його сторінки.

Розроблений сервіс в автоматичному режимі дозволяє перевірити більшість параметрів безпеки соціальних мереж Facebook та Instagram використовуючи їх API-функції та API-функції сервісу Have I Been Pwned.

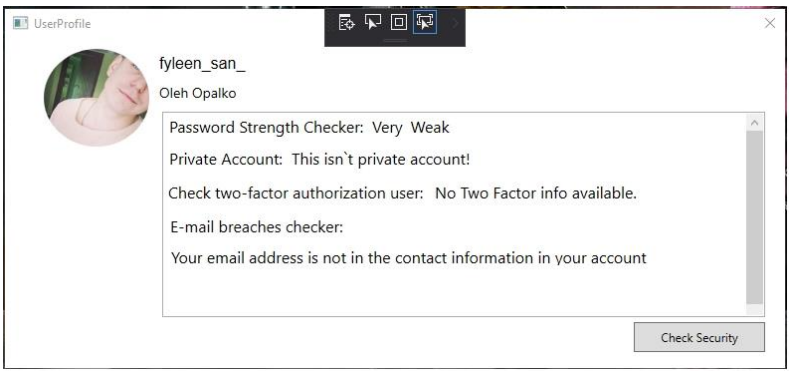

Рисунок 3 – Головне вікно програмного сервісу

У таблиці 1 подано результати порівняльного аналізу параметрів безпеки реалізовані у соціальних мережах та програмному сервісі.

Таблиця 1

Порівняльний аналіз параметрів безпеки реалізованих у програмному сервісі

Параметри безпеки сторінок	Реалізація у соціальній мережі		Реалізація у програмному сервісі	
	Facebook	Instagram	Facebook	Instagram
Двоетапна перевірка	+	+	-	+
Приватний обліковий запис	+	+	-	+
Сповіщення про безпеку та конфіденційність	+	-	-	-
Перевірка авторизованих входів	+	-	-	-
Формування довірених контактів	+	-	-	-
Генерування кодів ідентифікації	+	+	-	-
Перевірка складності пароля	+	+	+	+
Перевірка витоків пароля	-	-	+	+
Перевірка витоків даних для адреси електронної скриньки	-	-	+	+
Регулярна зміна пароля	-	-	-	-
Перевірка доступу зовнішніх застосунків до облікового запису	+	-	-	-

Висновок

У роботі спроектовано та реалізовано програмний сервіс для автоматичної перевірки параметрів безпеки персональних сторінок користувачів у соціальних мережах. Програмний сервіс дозволяє в автоматичному режимі перевірити наступні параметри безпеки: двоетапна перевірка, приватний обліковий запис, складність пароля, наявність витоків пароля та даних для адреси електронної скриньки.

Для реалізації використано середовище розробки Visual Studio Professional 2019, API-функції сервісу Have I Been Pwned, а також API-функції соціальних мереж Facebook та Instagram.

Список використаних джерел

1. R. McLeish, "YouTube accounts hacked by online security group", The Sydney Morning Herald, 2017, doi: http://www.smh.com.au/technology/technology-news/youtube-accounts-hacked-by-online-security-group-20170414-gvl31k.html
2. S. Clark, “Up to six million Instagram accounts affected by data breach”, The Stack, 2017, doi: https://thestack.com/security/2017/09/04/up-to-six-million-instagram-accounts affected -by-data-breach/.
3. R. Jabee, M.AfsharAlam, “Issues and Challenges of Cyber Security for Social Networking Sites (Facebook)”, International Journal of Computer Applications, vol. 144, No.3, pp. 36-40, 2016.
4. До 50 млн акаунтів в Facebook зламані невідомими хакерами [Електронний ресурс] Режим доступу – https://znaj.ua/techno/176920-pid-zagrozoyu-50-mln-koristuvachiv-facebook-popered iv-pro-strashnu-nebezpeku
5. R. Shevchuk, Y. Pastukh “Improve the Security of Social Media Accounts” in Proc. of 2019 9th International Conference on the Advanced Computer Information Technologies (ACIT-2019), Ceske Budejovice, Czech Republic, pp. 439–442, June 2019.
6. Пастух Я.Т. Засоби контролю безпеки облікових записів користувачів у соціальних мережах / Я.Т. Пастух // Матеріали
7. Семінару “Комп’ютерні науки та інформаційні технології”. — Тернопіль : ФО-П Шпак В.Б., 2018. — С. 51 – 52.
8. T. Hunt. FAQs: Need to know something about Have I Been Pwned. [Online]. Available: https://haveibeenpwned.com/
9. Facebook for developers. Facebook API [Online]. Available: https://developers.facebook.com