УДК 681.003

АРХІТЕКТУРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОЦІНКИ РІВНЯ ЗАХИСТУ КОРИСТУВАЧІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

Якимів А.Р.
Західноукраїнський національний університет
магістрант

I. Вступ

Сьогодні в теорії та практиці захисту персональних сторінок користувачів у соціальних мережах залишилось чимало не вирішених проблем[1-6]. Зокрема, відсутня класифікація загроз для користувачів соціальних мереж. Існуючі контролі безпеки для сторінок користувачів у соціальних мережах не в повній мірі забезпечують захист облікових записів [5,6]. Відсутні моделі оцінки рівня безпеки персональних сторінок користувачів у соціальних мережах, які б враховували рекомендовані фахівцями із інформаційної безпеки засоби контролю [1]. Як наслідок, гостро постає питання розробки програмного забезпечення для підвищення рівня безпеки персональних сторінок користувачів у соціальних мережах.

II. Мета роботи

Метою роботи є розробка архітектури програмного забезпечення для автоматичної оцінки рівня захисту користувачів у соціальних мережах.

III. Архітектура програмного забезпечення

У роботи виділено засоби контролю безпеки облікових записів користувачів у соціальних мережах Facebook, YouTube та Instagram та розроблено архітектуру програмного забезпечення для автоматичної оцінки рівня захисту користувачів у соціальних мережах (див.рис. 1).

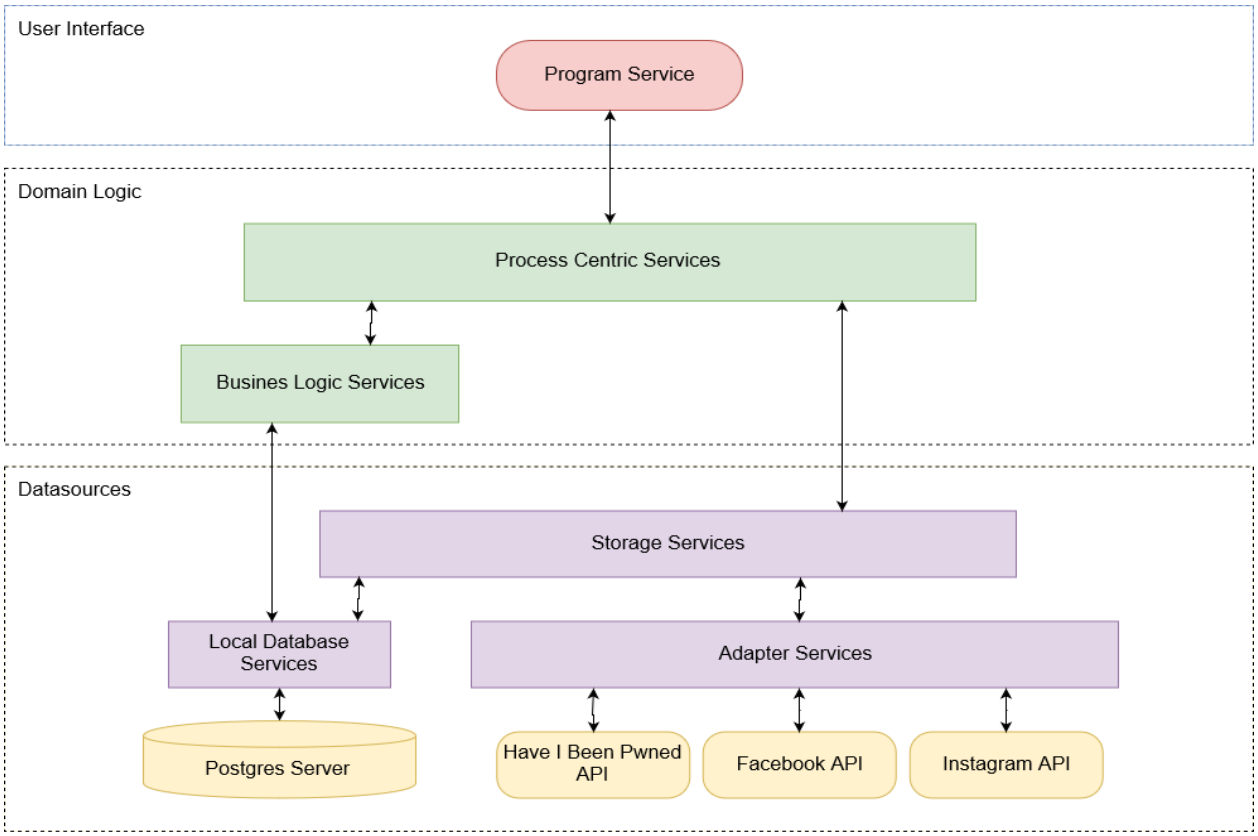

Рисунок 1 – Архітектура програмного забезпечення

Запропонована архітектура програмного забезпечення включає в себе три основних рівні, кожен з яких відіграє важливу роль у функціонуванні системи:

- UserInterface (Інтерфейс користувача): Цей рівень відповідає за графічний інтерфейс користувача.
- Domain Logic (Логіка області): На цьому рівні реалізована структурна та алгоритмічна складова програмного сервісу. Модуль Business Logic Services відповідає за логіку виконання запитів до бази даних. Модуль Process Centric Services керує логікою виконання запитів до модулів Business Logic Services та StorageService.
- Datasources (Джерела даних): Цей рівень представлений базами даних та взаємодіючими з ними модулями. Модуль Storage Services відповідає за аналіз та запис даних з особистої сторінки користувача у базу даних PostgresServer. LocalDatabase Services - це локальні служби баз даних, які використовуються для аналізу вхідних даних у Storage Services та подальшого їх запису в базу даних. Модуль Adapter Services отримує та конвертує дані з серверів, на яких реалізовані API-функції соціальних мереж (Facebook API, Instagram API), а також API функцій сервісу Have I BeenPwned.

Запропонована архітектура надає кілька ключових переваг при реалізації програмного забезпечення:

- Розділення бізнес-логіки на модулі Business Logic Services та Process Centric Services дозволяє ефективно керувати виконанням запитів до бази даних та логічними операціями в системі. Це робить систему гнучкою та легко розширюваною.
- Рівень Datasources раціонально використовує бази даних та модулі для ефективного аналізу, зберігання та обробки даних. Використання локальних служб баз даних та Adapter Services для взаємодії зі сторонніми API дозволяє розширювати можливості системи без великих змін в існуючій структурі.
- Існування чітко визначених меж між рівнями дозволяє вести розробку та тестування незалежно від інших частин системи, що робить код більш надійним.
- Модульна структура архітектури дозволяє легко додавати новий функціонал чи вносити зміни в існуючий, не впливаючи на решту системи, що робить систему більш гнучкою та готовою до реінженерії.

Висновок

Розробка та впровадження програмного забезпечення для автоматичної оцінки рівня захисту користувачів у соціальних мережах має велике значення в умовах постійно зростаючих загроз кібербезпеки.

Архітектура програмного забезпечення, яку було розроблено у роботі, представляє собою систему, що дозволяє автоматично оцінювати та аналізувати рівень захисту облікових записів у соціальних мережах. Ця архітектура визначає три ключові рівні: інтерфейс користувача, логіку області та джерела даних. На рівні інтерфейсу користувача забезпечується простий та зрозумілий інтерфейс, що спрощує взаємодію користувача з програмою. Логіка області включає модулі, які відповідають за алгоритмічні та структурні аспекти функціонування програмного сервісу. Джерела даних об'єднують бази даних, що використовуються для аналізу та збереження інформації з соціальних мереж.

Список використаних джерел

1. Computational Social Networks: Security and Privacy. [Електронний ресурс] / [M. Salama, M. Panda, Y. Elbarawyтаін.] // Computational Social Networks. – 2012. – Режим доступу до ресурсу : http://njtech.findplus.cn
2. Скрута Г.В. Забезпечення інформаційної безпеки у соціальних мережах / Скрута Г.В., Шкарупа І.В., Нікуліщев Г.І. // Актуальні задачі та досягнення у галузі кібербезпеки: Всеукраїнська науково-практична конференція студентів і молодих вчених, 23-25 листопада 2016 р. : матеріали конф. – Кропивницький, 2016. – С.79.
3. Карманний Є. В. Підходи до захисту інформації при користуванні соціальними мережами [Електронний ресурс] / Є. В. Карманний, С. О. Ковжога. – 2015. – Режим доступу до ресурсу : http://dspace.nlu.edu.ua/bitstream/ 123456789/8420/1/Karmannuy_Kovgoa.pdf.
4. K. Thomas, A. Moscicki (2019) New research: How effective is basic account hygiene at preventing hijacking [Online]. Available: https://security.googleblog.com/2019/05/new-research-how-effectiveis-basic.html
5. Cyber Security Guidelines for Securing Social Media Accounts (2018) [Online]. Available: https://www.qcert.org/sites/default/files/public/documents/guidelines_ for_securing_social_media_accounts.pdf
6. Identity Awareness, Protection, and Management Guide (2018). [Online]. Available: https://www.dla.mil/Portals/104/Users/230/98/