DOI 10.15276/imms.v15.no2.229
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 2, pp. 229-239

РОЗРОБКА ЗАСТОСУНКУ ДЛЯ ПОШУКУ ПРОФІЛІВ КОРИСТУВАЧІВ У СОЦІАЛЬНИХ МЕДІА ЯК ПОЧАТКОВИЙ ЕТАП OSINT-ДОСЛІДЖЕННЯ

А.В. Котляров, Н.І. Кушніренко, В.О. Назаров

Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Email: kushnirenko@op.edu.ua

У статті розглянуто розробку застосунку для пошуку профілів користувачів у соціальних медіа в контексті OSINT-дослідження. Досліджено основні типи ідентифікаторів користувачів, за якими можна здійснювати такий пошук, зокрема: номер телефону, адреса електронної пошти, зображення, прізвище та ім'я, нікнейм. Детально проаналізовано переваги та обмеження кожного з цих ідентифікаторів. Розроблено та описано алгоритми автоматизованого пошуку за прізвищем та ім'ям, а також за нікнеймом з відповідними блок-схемами. Описано основні технічні проблеми, що виникають при автоматизації процесу, включаючи обробку CAPTCHA, і запропоновано шляхи їх вирішення за допомогою бібліотеки Selenium WebDriver, що дозволяє емулювати дії реального користувача. На основі розроблених алгоритмів створено програмний застосунок "KotOSINT" мовою Python з графічним інтерфейсом на основі Tkinter. Застосунок забезпечує функціонал пошуку профілів користувачів у різних соціальних медіа, можливість додавання нових платформ, збереження історії пошуків та їх експорт. Проведено тестування, яке показало середній час перевірки одного посилання близько 4,2 секунди, що свідчить про ефективність застосунку.
Надано практичні рекомендації щодо безпечного використання розробленого інструменту, зокрема щодо застосування VPN, створення окремих профілів браузера з фейковими акаунтами, врахування мовних налаштувань системи та попереднього тестування в режимі перевірки. Застосунок "KotOSINT" має потенціал стати важливим інструментом у протидії кіберзлочинності та підвищенні ефективності OSINT-дослідження у сучасному інформаційному середовищі, де соціальні медіа відіграють ключову роль у комунікації та поширенні інформації. Розробка подібних інструментів є особливо актуальною в контексті збільшення кіберзагроз та необхідності розвитку засобів цифрової розвідки.
Ключові слова: OSINT, соціальні медіа, браузер, профіль користувача, нікнейм, Selenium.

Вступ. У сучасному цифровому світі соціальні медіа стали невід'ємною частиною повсякденного життя мільярдів людей, забезпечуючи швидку комунікацію та соціальну взаємодію. За даними Statista, станом на 2024 рік понад 5 мільярдів людей у світі користуються ними, що становить майже 62% глобального населення, і очікується, що до 2028 року ця кількість зросте до понад 6 мільярдів користувачів. При цьому середня тривалість щоденного користування становить 151 хвилину [1].

Соціальні медіа – це вид масмедіа, побудованих на ідеологічних та технологічних принципах Web 2.0. Перші соціальні медіа почали з'являтися ще у 1990-х роках, проте основний етап їх розвитку розпочався у 2004 році, коли Тім О'Рейлі опублікував статтю "What Is Web 2.0", що окреслила ключові принципи нової цифрової епохи [2]. Зараз соціальні медіа охоплюють широкий спектр ресурсів, які умовно можна поділити за їхнім призначенням на такі типи: соціальні мережі, медіа-платформи, блоги, форуми, освітні ресурси, месенджери, платформи для знайомств, вікі-проєкти та віртуальні ігрові світи [3].

Проте соціальні медіа, у поєднанні з анонімністю, стали основним середовищем для здійснення кіберзлочинів. Серед прикладів такого використання – пропаганда, тероризм, наркоторгівля, шахрайство, порнографія, піратство, кібербулінг. Водночас

особливою загрозою сьогодення є їхнє використання у військовому контексті, що може призвести до витоку критично важливої інформації та поставити під загрозу національну безпеку [4].

У боротьбі з цими загрозами важливу роль відіграє OSINT (Open Source Intelligence), який є одним із трьох ключових напрямів сучасної розвідки. Під OSINT розуміють збір, оцінку та аналіз інформації із загальнодоступних джерел (як платних, так і безкоштовних) з метою їх використання як розвідданих або доказів [5]. Засновником даної технології вважається Шерман Кент, який тривалий час працював в Центральному розвідувальному управлінні (ЦРУ). Саме під його керівництвом був створений «Єльський звіт», який спричинив неабиякий резонанс у наукових та військових колах. Документ оцінював, яку інформацію про боєготовність американських збройних сил противник міг зібрати з відкритих джерел. В результаті понад 90% зібраної інформації виявилась правдивою [6].

Застосування OSINT має низку важливих переваг порівняно з іншими видами розвідки, зокрема: простоту отримання інформації, швидкість збору та аналізу даних, безпеку розслідувань, економічну ефективність та можливість моніторингу в реальному часі. Що робить його надзвичайно цінним для правоохоронних органів, журналістів, військових та інших спеціалістів із кібербезпеки. Зважаючи на це, виникає потреба у розробці спеціалізованих застосунків, які дозволятимуть здійснювати пошук потенційних зловмисників за їхніми цифровими слідами.

Мета і задачі дослідження. Метою роботи є розробка застосунку для пошуку профілів користувачів у соціальних медіа, що дозволить ефективно виявляти можливі профілі реальних злочинців. Для досягнення поставленої мети були визначені наступні задачі:

- дослідити основні типи ідентифікаторів користувачів;
- розробити алгоритм пошуку профілів користувачів у соцмедіа;
- реалізувати застосунок, на основі даного алгоритму,
- провести тестування застосунку та надати рекомендації щодо використання.

Основна частина. Для пошуку інформації в соціальних медіа потрібна відправна точка – початкові дані, за якими здійснюватиметься пошук. Найважливішими серед них є ідентифікатори – унікальні або частково унікальні відомості, що дозволяють точно визначити особу або звузити коло пошуку. Основними відомостями, за якими можна знайти профілі в соціальних медіа, є:

- номер телефону;
- адреса електронної пошти;
- зображення;
- прізвище та ім’я;
- нікнейм.

Перші два відносяться до категорії чітких ідентифікаторів, оскільки дозволяють однозначно встановити зв’язок між різними обліковими записами користувача. Це зумовлено тим, що вони є унікальними для кожного користувача, адже використовуються в процесі реєстрації або авторизації в соцмедіа і не можуть повторюватися іншими користувачами. Однак у більшості випадків ці ідентифікатори не відображаються відкрито на самій платформі, що обмежує їх використання для пошуку. Проте навіть якщо це можливо, користувач може обмежити видимість цих даних у налаштуваннях конфіденційності. Прикладами є месенджери Telegram і Viber, в яких можна знайти профіль користувача, якщо додати його номер до списку контактів. Нажаль повноцінна автоматизація цього процесу ускладнюється через високу ймовірність блокування.

У зв’язку з обмеженими технічними можливостями відкритого пошуку за цими ідентифікаторами, на практиці вони найчастіше застосовуються для пошуку в DarkNet, зокрема по злитих базах даних. Хоча такі джерела також можуть використовуватись в

OSINT, у межах даної статті подібні методи не реалізовуватимуться з огляду на їхню сумнівну законність та невідповідність етичним принципам.

Наступним розглянемо – зображення. Воно не є настільки чітким ідентифікатором, як попередні, особливо у випадках, коли зображення не є особистим. Навіть якщо на фотографії присутнє обличчя, це не завжди дозволяє достовірно встановити зв'язок із певним профілем, оскільки користувач може завантажити будь-яке зображення у власний обліковий запис.

Ще одна проблема полягає в тому, що соцмедіа не мають вбудованої можливості пошуку за зображеннями. Натомість існують сторонні сервіси, що мають величезні власні бази даних із застосуванням складних алгоритмів розпізнавання облич. Через те, що ці інструменти працюють незалежно від самих соцмедіа і спираються на власні технології, реалізація пошуку за таким типом ідентифікатора не розглядатиметься в даній роботі. Проте варто знати, що такі сервіси, як Google Images, PimEyes і Betaface, є корисними у процесі OSINT-дослідження.

Розглянемо пошук за прізвищем та ім'ям (далі ПІ). ПІ є однією з найочевидніших та найпростіших точок входу для пошуку профілів. Це пояснюється тим, що під час реєстрації всі платформи вимагають вказувати їх, і вони завжди залишаються відкритими для перегляду, навіть якщо профіль повністю закритий.

Однак слід зазначити, що такий пошук не є чітким, оскільки в соціальних медіа може існувати безліч людей із таким самим прізвищем та ім'ям. Зрозуміло, що чим більш рідкісне ПІ тим менша кількість таких профілів, що полегшує подальшу ідентифікацію особи. Ще однією проблемою є різні варіації написання, пов'язані з скороченням, транслітерацією, перекладом та заміною символів.

Тим не менш, використання цього ідентифікатора дозволяє визначити хоча б те, чи є на певній платформі користувач із такими даними.

Щоб здійснити пошук профілю «вручну», достатньо скористатися вбудованим пошуком в будь-якій соцмедіа. Для цього потрібно лише ввести ім'я та прізвище у відповідне пошукове поле, а потім переглянути результати. Якщо потрібно, скористатися фільтрами.

Автоматизувати пошук за цим ідентифікатором можна через використання пошукових URL в самих соціальних медіа. Наприклад, для LinkedIn використовується формат – «https://www.linkedin.com/search/results/people/?keywords={}». Куди замість символів «{}» підставляється будь-яке ПІ. Для визначення наявності профілю буде здійснюватися пошук певної фрази-помилки на сторінці. У випадку LinkedIn це фраза «No results found». Якщо цей текст присутній у відповіді сервіса, це означає, що профілів із такими даними не знайдено. Але також слід враховувати мову, на якій будуть відображатися дані фрази. На рисунку 1 зображено блок-схему алгоритму пошуку за ПІ у розроблюваному застосунку.

Ще одним видом пошуку є пошук за Нікнеймом. Нікнейм (від англ. nickname – прізвисько) – це вигадане ім'я, яке користувач використовує в соціальних медіа. Зазвичай воно походить від власного імені чи прізвища, може бути натхненне вигаданими персонажами, відомими особистостями або мати інше значення, яке пов'язане з власником. У соцмедіа нікнейм виконує функцію унікального ідентифікатора користувача, замінюючи числовий ID. Це забезпечує зручність у спілкуванні та взаємодії, адже запам'ятати нікнейм набагато простіше, ніж довгий набір цифр. Завдяки тому, що на одній платформі кожен нікнейм є унікальним, він забезпечує більш точну ідентифікацію профілю порівняно з ПІ. Водночас існує ймовірність, що той самий нікнейм буде використаний іншою особою на іншій платформі. Також є проблема з можливістю його зміни на інший, що може викликати додаткові труднощі.

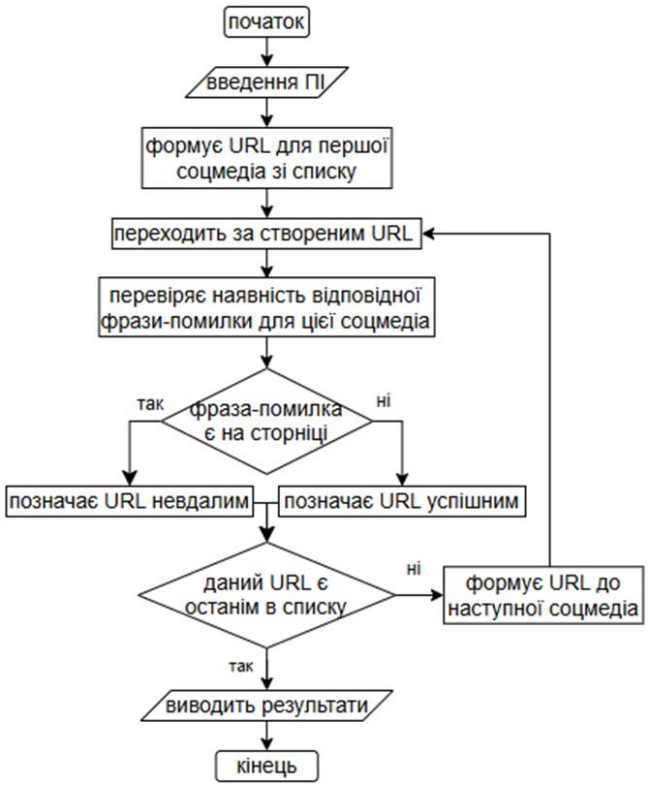

Рис. 1. Блок-схема алгоритму пошуку за прізвищем та ім’ям

Для багатьох користувачів характерна лінь, що проявляється у небажанні створювати окремі нікнейми для кожної соціальної медіа – аналогічна поведінка спостерігається і щодо паролів. Цей фактор, поряд із прагненням до зручності, призводить до повторного використання одного і того самого нікнейму на різних платформах.

Частою також є практика використання частини перед «@» в адресі електронної пошти. Наприклад, якщо суб’єкт використовує «mpulido007@gmail.com», то існує велика ймовірність, що він може використовувати «mpulido007» як псевдонім в якійсь із соціальних медіа [7].

Здійснення пошуку «вручну» за нікнеймом є подібним до пошуку за прізвищем та ім’ям: користувач вводить запит у пошукове поле в соцмедіа та отримує результат. Проте слід враховувати, що не всі підтримують пошук саме за нікнеймом.

Автоматизувати пошук можна два способами. Перший – простіший у реалізації, відповідно більш швидший. Зазвичай використовується лише бібліотека Requests, яка дозволяє отримувати HTTP-статус сторінки. Якщо код 2xx, то профіль існує, якщо 4xx то ні. Однак у цього метода проблеми з надійністю перевірки, оскільки не всі соцмедіа повертають 4xx навіть у разі відсутності користувача, а замість цього вони можуть просто перенаправляти запит на головну сторінку або ж повертати код 200 з відображенням текстової помилки (так звана м'яка помилка 404 – soft 404). Через це алгоритм може помилково вважати, що профіль існує, коли насправді його немає.

Другий спосіб повільніший, однак майже стовідсотково визначить чи є профіль в конкретній соцмедіа чи ні. Цей спосіб базується на поєднанні бібліотек Requests та BeautifulSoup. Спочатку Requests визначає HTTP-статус, при цьому додатково проводиться перевірка на 3xx коди, тобто на перенаправлення на іншу сторінку. Після цього, якщо отримано код 2xx, BeautifulSoup починає шукати відповідну фразу-помилку на сторінці.

Прикладом реального застосунку, який використовує подібний алгоритм пошуку є Sherlock [7]. Розроблюваний застосунок також буде використовувати вище наведений алгоритм. На рисунку 2 зображена схема алгоритму за нікнеймом.

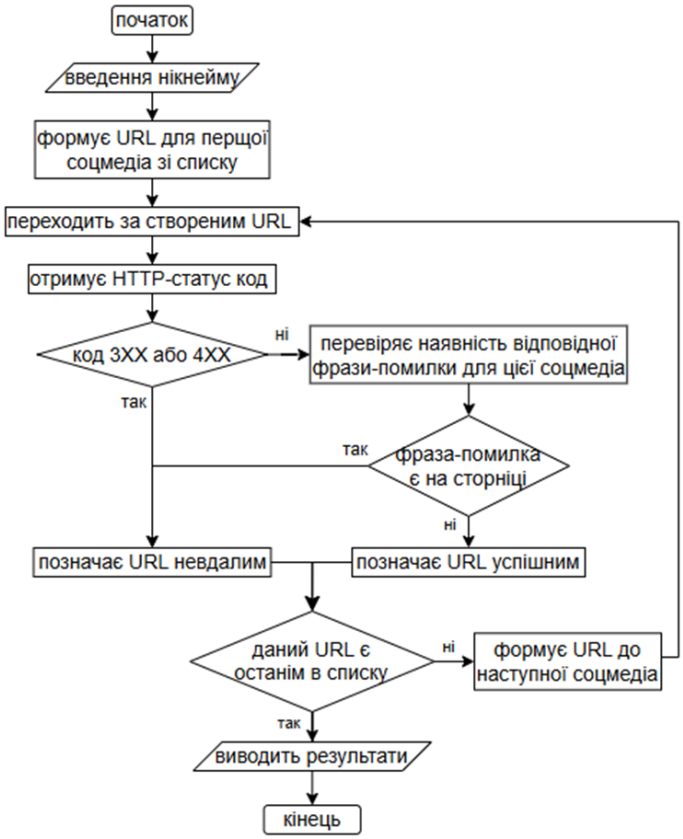

Рис. 2. Блок-схема алгоритму пошуку за нікнеймом

Отже, розроблюваний застосунок реалізовуватиме механізми пошуку за двома типами ідентифікаторів користувача – прізвищем і ім'ям, а також за нікнеймом.

Водночас описані вище алгоритми для обох типів, мають спільне суттєве обмеження – вони не передбачають обробку CAPTCHA, що є важливою перешкодою для автоматизації процесу. CAPTCHA – це технологія, призначена для відокремлення людських користувачів від автоматизованих ботів. Найпоширенішим методом їх автоматизованого вирішення є використання онлайн-сервісів розв'язання CAPTCHA. Інший метод передбачає використання ротації IP-адрес. Однак дані методи не є безкоштовними [8].

Існує ще один метод, який дозволить зменшити ймовірність появи CAPTCHA майже до нуля. Якщо ж вона навіть з'явиться, то перевірка на існування профілю відбудеться швидше за її появу. Реалізується це за допомогою бібліотеки Selenium WebDriver – це комплексний набір інструментів для автоматизації взаємодії з веб-браузерами, що дозволяє програмно керувати поведінкою браузера, імітуючи дії користувача на веб-сторінках. Тобто сайт сприйматиме запити від застосунку як звичайну активність реального користувача, а не як автоматизований скрипт.

Водночас можливе використання будь-якого браузерного профілю, а не лише гостьового режиму. Це відкриває додаткові можливості для обходу обмежень, пов'язаних із необхідністю обов'язкової авторизації у деяких соціальних медіа, без якої доступ до певного контенту є неможливим. Завдяки використанню збережених облікових даних у профілі браузера, автоматизована система може діяти від імені реального користувача, що дозволяє уникнути появи сторінок авторизації.

Тому саме цей метод обрано для розроблюваного застосунку.

Однак даний підхід не позбавлений певних недоліків. По-перше, використання Selenium WebDriver створює додаткове навантаження на обчислювальні ресурси системи. По-друге, загальний час виконання перевірок суттєво зростає. І останній,

найбільш суттєвий недолік – це потенційна загроза конфіденційності. Оскільки Selenium WebDriver має доступ до всього функціоналу браузера, автоматизована програма може, прямо чи опосередковано, отримати доступ до чутливої інформації. У випадку компрометації такого коду, це може створити ризик витоку даних користувача. Водночас, це питання легко вирішується – достатньо попередньо створити окремий браузерний профіль без будь-яких чутливих даних із фальшивими обліковими записами для входу у необхідні соцмедіа. Таким чином, користувач може підготувати середовище для запуску заздалегідь і не перейматися за свою конфіденційність, повністю контролюючи, які саме дані використовуються під час роботи застосунку. Додатково можна використовувати VPN. Проте, для досягнення максимального рівня безпеки, рекомендується поєднувати зазначені заходи з ізоляцією середовища запуску.

Розроблюваний застосунок має назву «KotOSINT». За замовчуванням у застосунку передбачено наявність 50 URL для пошуку за нікнеймами та 25 – для пошуку за ПІ. Кожен з них супроводжується відповідними фразами-помилками англійською та українською мовами.

У якості основної мови програмування обрано Python, через його зрозумілий синтаксис та розвинену екосистему бібліотек. Середовищем розробки є PyCharm. Для побудови графічного інтерфейсу використано бібліотеку Tkinter.

Для збереження даних прийнято рішення використовувати JSON-файли замість традиційної бази даних. Це зумовлено низкою факторів, серед яких невеликий обсяг даних, їх простота та відсутність необхідності в складних структурах або взаємозв'язках. Тому використання традиційної бази даних було б надмірним для такого застосунку. Однак при потребі структура JSON дозволяє без зусиль перенести дані до низки сучасних СУБД, зокрема таких як MongoDB, PostgreSQL або SQLite [9]. На рисунку 3 представлена іконка файлу запуску програми (batch-файл).

Рис. 3. Вигляд іконки файлу запуску застосунку

Після запуску batch-файлу відкриється вступне вікно (вкладка «Головна»), де представлено основні можливості застосунку. У цьому ж вікні зазначено контакт для зв'язку з розробником у разі виникнення питань. Дане вікно зображено на рисунку 4.

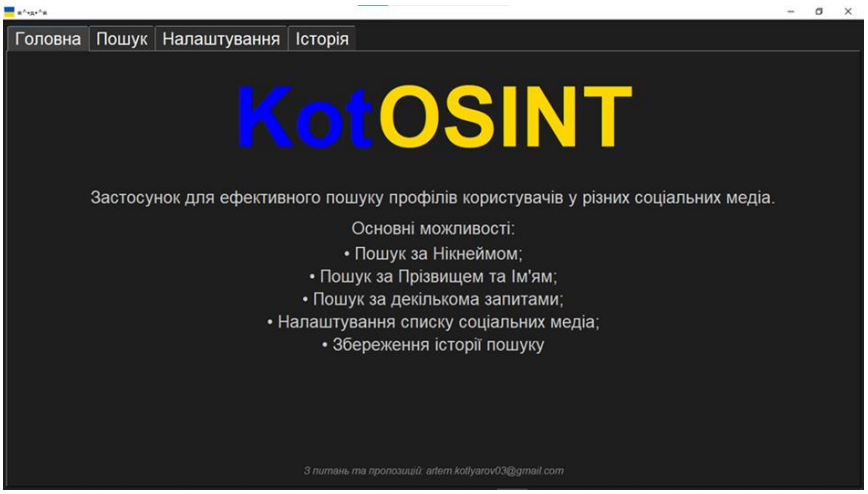

Рис. 4. Вступне вікно застосунку

Вкладка «Налаштування» має три розділи: «Профіль браузера», «URL для Нікнеймів» та «URL для ПІ».

У розділі «Профіль браузера» користувач має змогу вибрати бажаний браузер (Chrome, Edge, Firefox) і вказати назву профілю. Після цього достатньо натиснути кнопку «Зберегти». Обрані параметри будуть збережені, тож при наступних запусках програми їх не доведеться вводити знову. Якщо цього не зробити, то запуститься браузер Edge з Default профілем. На рисунку 5 зображено даний розділ.

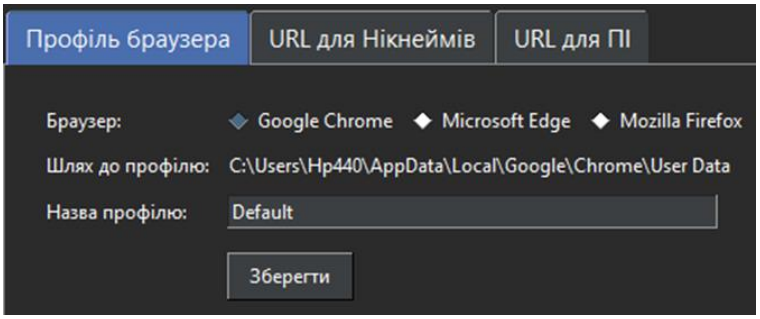

Рис. 5. Розділ обрання профілю браузера

Розділи «URL для Нікнеймів» та «URL для ПІ» загалом схожі. У верхній частині в обох розташована форма для додавання нових соціальних медіа. Де потрібно ввести: назву соцмедіа, URL (обов'язково із символами {}) та фрази-помилки (для ПІ це обов’язково). На рисунку 6 зображено ці форми з відповідними параметрами.

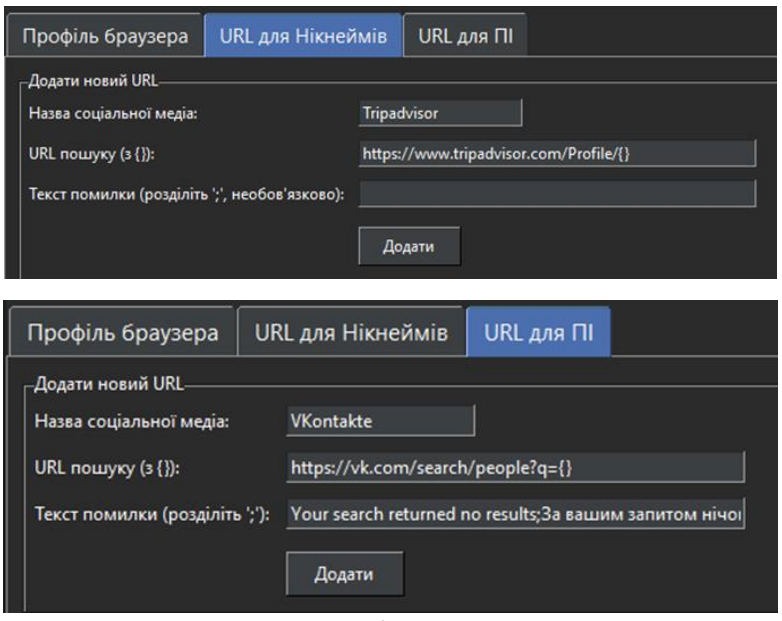

Рис. 6. Форми для додавання нових соцмедіа

Після натискання на кнопку «Додати» ці URL з’являться у списках, що знаходяться у нижній частині розділів. Якщо натиснути двічі на певний запис, то відкриється вікно редагування, де користувач може змінити будь-який параметр. Також, за необхідності, їх можна видаляти натисканням правої клавіші миші,.

Вкладка «Пошук» складається з двох частин. У правій частині, розміщено списки соціальних медіа, де можна вибрати потрібні варіанти, активуючи відповідні мітки. Для спрощення процесу вибору є кнопки «Вибрати всі» та «Зняти вибір» Крім того, реалізовано функціонал перетягування елементів у списку. Після вибору необхідних пунктів або всіх одразу слід натиснути кнопку «Зберегти». Якщо не вибрати жодного, то

під час спроби виконати пошук з’явиться повідомлення про помилку. На рисунку 7 зображено частину одного зі списків.

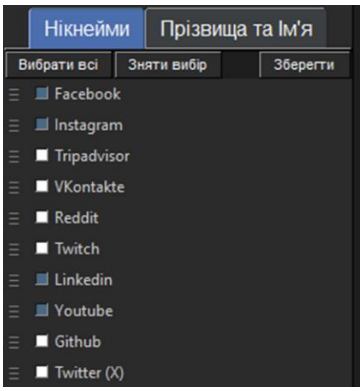

Рис. 7. Частина списку вибору соціальних медіа

У лівій частині даної вкладки знаходиться головні елементи інтерфейсу пошуку:

- кнопки вибору типу пошукового запиту («За Нікнеймом» або «За ПІ»);
- поле для введення цього запиту;
- кнопка для додавання додаткових полів введення (максимум 10), а також їх видалення;
- мітка «Режим перевірки», яка визначає чи виконуватиметься пошук у фоновому режимі, чи у інтерактивному режимі;
- кнопка «Пошук», яка розпочинає пошук;
- кнопка «Зупинити», яка зупиняє пошук в аварійному режимі;
- прогрес-бар, що відображає стан пошуку;
- поле для виведення отриманих результатів.

Для прикладу виберемо пошук за Нікнеймом та задамо такі значення: MaxTech01, MaxTech02, MaxTech03. Використаємо список соцмедіа, наведений на рисунку 7. Натискаємо на кнопку «Шукати». Після виконання пошуку отримуємо результат, що зображено на рисунку 8.

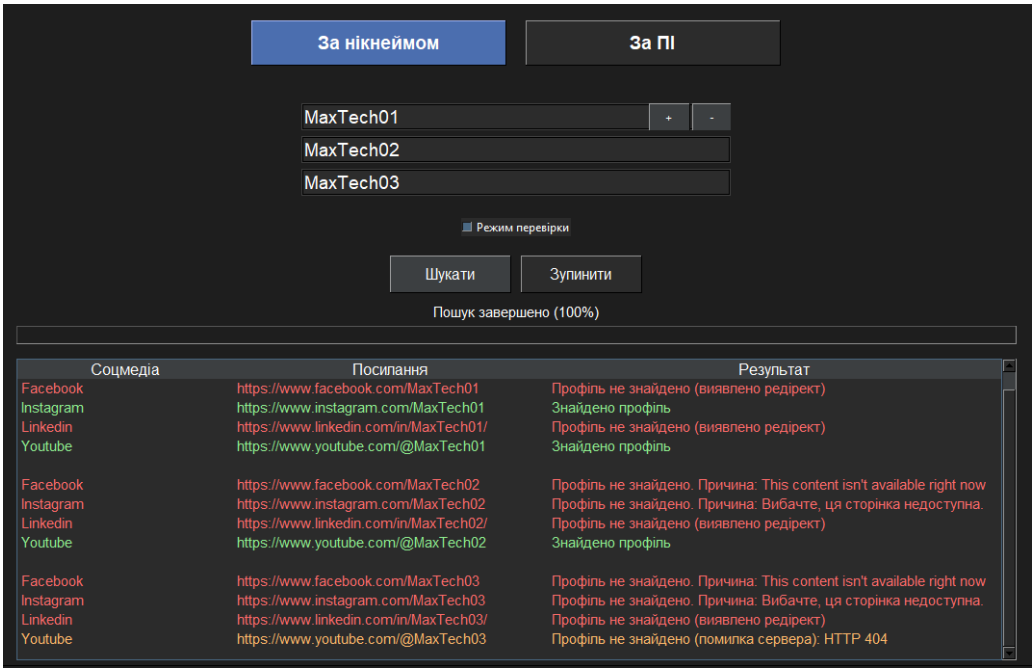

Рис. 8. Результати пошуку

Вкладка «Історія», відображає журнал попередніх пошукових запитів, що дозволяє користувачеві переглядати результати, отримані під час попередніх сеансів роботи із застосунком. Вона впорядкована за часом, тобто: найновіші результати розміщуються у верхній частині списку, тоді як більш давні – у нижній. На рисунку 9 зображено дану вкладку.

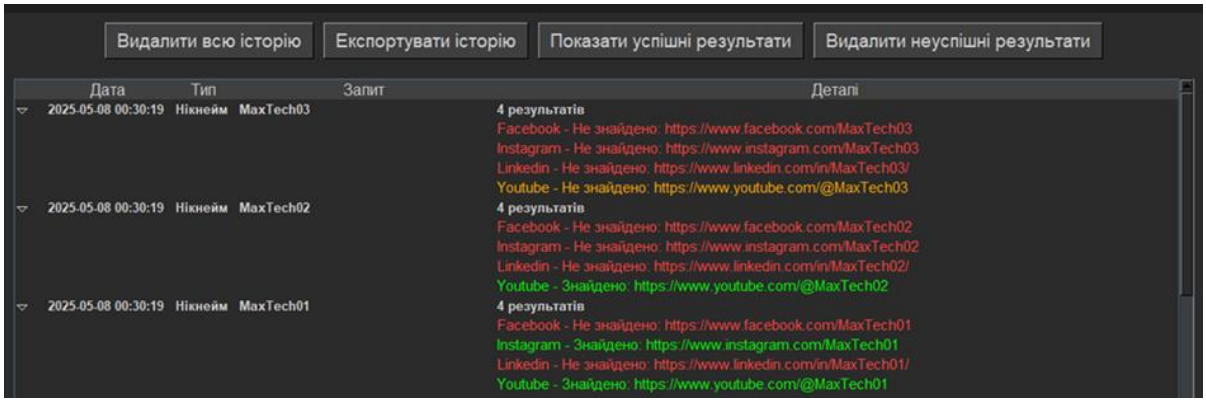

Рис. 9. Вкладка «Історія»

У верхній частині вкладки розміщені кнопки для виконання певних дій над історією, серед яких:

– «Видалити усі результати» – виконує повне очищення історії без можливості відновлення;

– «Показати успішні результати» – фільтрує записи, внаслідок чого на екрані відображаються лише успішні;

– «Видалити неуспішні результати» – виконує безпосереднє видалення всіх неуспішних записів з історії.

– «Експортувати історію» – генерує файл у форматі Excel та автоматично завантажує його на комп’ютер користувача.

Додатково, користувач має можливість видаляти окремі записи з історії – для цього достатньо натиснути правою кнопкою миші на обраному записі та вибрати пункт «Видалити запис».

Щодо тривалості пошуку, результати якого наведено на рисунку 8, варто зазначити, що весь процес зайняв 55 секунд і складався з двох основних етапів. Зокрема, 5 секунд було витрачено на запуск браузера, а решту часу – 50 секунд – було витрачено на перехід за посиланнями та їх аналіз. При цьому усього перевірено 12 посилань.

Для оцінки ефективності роботи системи доцільно розрахувати середній час перевірки одного посилання – t. Цей показник можна обчислити, поділивши час, витрачений на перевірку (без урахування часу запуску браузера) – T, на кількість перевірених посилань N. У даному випадку: $t = T / N = 50 / 12 \approx 4.2$ секунди. Що є досить гарним результатом.

Слід зазначити, що швидкість обробки запиту різниться залежно від ситуації. У випадку отримання негативного HTTP-статус коду, перевірка відбудеться майже миттєво. Навіть при успішному існує певна невизначеність щодо часу обробки. Якщо система знаходить фразу-помилку на початку сторінки, це відбувається швидше, ніж коли така фраза розташована в кінці. А якщо фраза-помилка взагалі відсутня, то процес займе ще більше часу, оскільки програмі необхідно проаналізувати весь вміст сторінки.

Окрім безпосередньої розробки застосунку, було також підготовано набір рекомендації для користувачів щодо його ефективного використання.

По-перше, необхідно використовувати VPN, що працює на рівні всієї системи, а не як розширення браузера. Це необхідно не лише для забезпечення безпеки, але й для отримання доступу до ресурсів, які були заблоковані відповідно до Указу Президента

України №133/2017 «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [10]. У сучасних умовах такі ресурси мають величезне значення для OSINT.

По-друге, створити окремий профіль у браузері, що дозволяє уникнути змішування особистої інформації з даними, що використовуються в дослідженнях. Також у межах цього профілю необхідно створити фейкові акаунти в різних соціальних медіа. Це особливо важливо, оскільки деякі платформи можуть виявити підозрілу активність і заблокувати особистий акаунт через сприйняття його як бота. Крім того, є певні ресурси, що можуть показувати іншим користувачам, хто переглядав їх акаунт, що створює ризик для анонімності.

По-третє, необхідно враховувати мову інтерфейсу. Застосунок за замовчуванням розпізнає повідомлення про помилки у соцмедіа лише українською та англійською мовами. Тому для коректного визначення наявності чи відсутності профілю бажано, щоб мовні налаштування системи відповідали одній із цих мов. Якщо ж користувач працює з іншим мовним інтерфейсом, є два варіанти: або вручну додати відповідні фрази до налаштувань застосунку, або змінити мову інтерфейсу кожної соцмедіа на англійську або українську. Важливо: обов'язково вимкнути функцію автоматичного перекладу сторінок у браузері.

По-четверте, перший запуск застосунку слід виконувати у режимі перевірки. Це дозволяє протестувати роботу системи та переконатися, що всі попередні налаштування здійснено коректно: створено відповідний профіль у браузері з фейковими акаунтами, обрана відповідна мова інтерфейсу, а також, за потреби, чи активовано VPN. Найважливіше – цей режим дає змогу впевнитися у правильності визначення наявності або відсутності профілю в соціальній медіа. Режим перевірки також доцільно використовувати при додаванні нових платформ до системи, щоб перевірити, як саме здійснюється пошук по ним.

Висновки. У рамках даної роботи було створено застосунок «KotOSINT», що призначений для автоматизованого пошуку профілів користувачів у соціальних медіа як початкового етапу OSINT-дослідження. У застосунку реалізовано два основні типи пошуку – за прізвищем та ім'ям (ПІ) і за нікнеймом, для яких наведено та описано відповідні алгоритми з детальними блок-схемами.

Застосунок реалізовано мовою програмування Python із використанням бібліотеки Tkinter для створення графічного інтерфейсу. Для збереження конфігураційних даних та результатів роботи обрано формат JSON, який забезпечує простоту структури та зручність подальшої інтеграції з повноцінними СУБД при потребі. Значною технічною перевагою застосунку є впровадження бібліотеки Selenium WebDriver, що забезпечує емуляцію дій реального користувача під час роботи в браузері. Це дозволяє ефективно обходити труднощі, пов'язані з появою CAPTCHA та необхідністю проходження авторизації.

У роботі також надано практичні рекомендації щодо безпечного та ефективного використання застосунку.

Тестування продуктивності розробленого застосунку засвідчило, що середній час перевірки одного посилання становить приблизно 4,2 секунди. Такий результат є достатньо високим для програмних засобів даного класу та підтверджує його практичну цінність. Отже, застосунок «KotOSINT» може істотно оптимізувати процес OSINT-досліджень і має потенціал стати дієвим інструментом у протидії кіберзлочинності.

Список літератури

1. Dixon S.J. Number of social media users worldwide from 2017 to 2028. URL: https://surl.lu/bsejrt
2. O'Reilly, T. What is Web 2.0: design patterns and business models for the next generation of software. O'Reilly Media, 2005. URL: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html

3. Aichner T., Jacob F. Measuring the degree of corporate social media use. International journal of market research. 2015. 57 p. DOI: https://doi.org/10.2501/IJMR-2015-018
4. Кучій О., Фролова О. Використання соціальних медіа як інструменту сучасної гібридної війни. *Acta de Historia & Politica: Saeculum XXI.* 2023. С. 93-104. DOI: https://doi.org/10.26693/ahpsxxi2023.si.093
5. Housego J. Guidance on open source investigation/research. London : National Police Chiefs' Council, 2020. 14 p.
6. Kent S. The Yale Report. 1951. 627 p. URL: https://www.cia.gov/resources/csi/static/The-Yale-Report.pdf
7. 27. Bazzell M. OSINT techniques: resources for uncovering online information: № 10. 2023. 550 p. URL: https://surl.li/rymyrr
8. Харченко В. О. Оцінювання вразливостей системи кіберзахисту на основі оптичного тесту Тюрінга CAPTCHA: дипл. … бак. : КПІ. Київ, 2021. 48 с.
9. Pranisha R. JSON vs SQL: What's the Difference? URL: https://olibr.com/blog/json-vs-sql-whats-the-difference/
10. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) : Рішення РНБО України від 15.04.2021 : станом на 23 квіт. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/n0030525-21#Text

DEVELOPMENT OF AN APPLICATION FOR SEARCHING USER PROFILES IN SOCIAL MEDIA AS THE INITIAL STAGE OF OSINT RESEARCH

A.V. Kotliarov, N.I. Kushnirenko, V.O. Nazarov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Email: kushnirenko@op.edu.ua

The article discusses the development of an application for searching user profiles in social media in the context of OSINT research. The main types of user identifiers by which such a search can be performed are studied, in particular: phone number, email address, image, last name and first name, nickname. The advantages and limitations of each of these identifiers are analyzed in detail. Algorithms for automated search by last name and first name, as well as by nickname with corresponding flowcharts are developed and described. The main technical problems that arise when automating the process, including CAPTCHA processing, are described, and their solution is proposed using the Selenium WebDriver library, which allows emulating the actions of a real user. Based on the developed algorithms, a software application "KotOSINT" was created in Python with a graphical interface based on Tkinter. The application provides the functionality of searching user profiles in various social media, the ability to add new platforms, save search history and export them. Testing was conducted, which showed an average time of checking one link of about 4.2 seconds, which indicates the effectiveness of the application. Practical recommendations are provided for the safe use of the developed tool, in particular, regarding the use of VPN, the creation of separate browser profiles with fake accounts, taking into account the language settings of the system and preliminary testing in the verification mode. The "KotOSINT" application has the potential to become an important tool in combating cybercrime and increasing the effectiveness of OSINT research in the modern information environment, where social media play a key role in communication and dissemination of information. The development of such tools is especially relevant in the context of increasing cyber threats and the need to develop digital intelligence tools.

Keywords: OSINT, social media, browser, user profile, nickname, Selenium.