Сябрук М. О., магістрантка,
Державний університет «Житомирська політехніка»

СИСТЕМА РОЗПІЗНАВАННЯ КОРИСТУВАЧІВ В СОЦІАЛЬНИХ МЕРЕЖАХ

За останні роки спостерігається стрімкий ріст кількості користувачів соціальних мереж по всьому світу. За даними Demandsage на кінець 2023 року користувачів соціальних мереж налічувалося близько 4,95 мільярдів, і прогнозується, що за 2024 рік їх кількість збільшиться до 5,17 мільярдів [1]. Через такі швидкі темпи розвитку соцмереж щодня генерується величезна кількість даних. На фоні такого розповсюдження і розширення виникають ризики, пов'язані з безпекою інформації, які стають складним завданням. Тому нам необхідне рішення безпеки, яке захистить користувачів, оскільки прості застосунки не мають необхідних мір для захисту персональної інформації користувача.

Таким рішенням безпеки може бути пропонована система розпізнавання доброякісного користувача в соціальних мережах від хакера. Отже, користувач заповнює свої дані і зберігає їх в захищеній базі даних, доступ до якої має тільки технічна підтримка, для використання в майбутньому. При наступному вході на дану платформу користувач вводить ці дані. Ця інформація проходить перевірку, тобто звіряється зі вже наявним ідентифікатором в базі даних. Якщо вона співпадає, то виконується вхід. Головним елементом такої системи є камера, яка фотографує користувача, якщо той вперше ввів неправильно пароль. В цій ситуації користувачу з невірними обліковими даними буде відмовлено у використанні платформи соціальної мережі, а наступним кроком інтегрована система відправить електронний лист зі зробленим фото реальному користувачу, якому належить профіль. Тоді він обирає варіант повторної спроби, якщо це, наприклад, він сам помилився, або відмови у доступі. Служба технічної підтримки теж отримає аналогічне попередження, яке надалі зможе передати у відповідні органи [2].

У великих компаніях зазвичай працюють команди, які підтримують свою присутність в кіберпросторі соцмереж, починаючи від створення публікацій, закінчуючи обміном повідомленнями між коллегами або відповідями клієнтам. Чим більше людей мають доступ до облікового запису, тим більша поверхня атаки і тим тяжче виявити, стримати і пом'якшити витік даних. Тому наявність однієї людини, яка буде відповідати за нагляд за соціальними мережами, може допомогти знизити ризики безпеки. В цьому, знову ж таки перевага пропонованої системи. Так як при доступі когось стороннього, існуючий користувач може виконати необхідні дії для протидії атаці [3].

Робочий механізм пропонованої системи показано на рисунку 1.

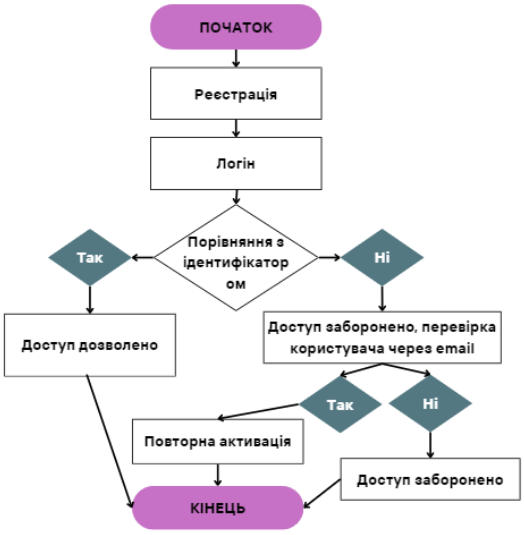

Рис. 1. Блок-схема пропонованої системи

Оскільки кіберзлочинці все частіше розробляють складні та нищівні атаки, платформи соціальних мереж повинні мати надійний захист на противагу. З цих міркувань було запропоновано систему – удосконалення вже наявних засобів захисту, яка захищає користувачів соціальних мереж та суттєво знижує ризики взлому їх профілів, а також дає можливість ідентифікувати порушника.

Список використаних джерел

1. Demandsage: Social Media Users 2024 (Global Data&Statistics). URL:https://www.demandsage.com/social-media-users/.
2. The Development of a Secure Online System to Protect Social Networking Platforms from Security Attacks / Basil Alothman: SpecialIssue «New Challengesin Cybe rSecurityandPrivacy». Kuwait, 2023.
3. UpGuard: The Impact of Social Media on Cybersecurity. URL: https://www.upguard.com/blog/the-impact-of-social-media-on-cybersecurity.