

# ВИЯВЛЕННЯ АГЕНТІВ ЗАГРОЗ КОНФІДЕНЦІЙНОСТІ НА ОСНОВІ МНОЖИНИ СПІЛЬНОТ СОЦІАЛЬНОЇ МЕРЕЖІ

Вінницький національний технічний університет;

## **Анотація**

*У доповіді розглянуто існуючі методи виявлення агентів загроз конфіденційності інформації з використанням соціальних мереж. Наведено попередні досягнення та перспективи розвитку напрямку.*

**Ключові слова:** загроза, агент, конфіденційність інформації, соціальна мережа.

## **Abstract**

*The report describes existing methods for identifying of privacy threats agents with using of the social networks. Earlier achievements and prospects of the development direction are specified.*

**Keywords:** threat, agent, information privacy, social network.

## **Вступ**

Економічна стабільність підприємства ґрунтується на ряді показників, серед яких є збереження конфіденційності, цілісності, доступності інформації, що пов'язана з його діяльністю. Технічні та програмні засоби не здатні повною мірою захистити від витіку інформації, оскільки неможливо повністю виключити людський фактор.

Соціальні мережі є невід'ємною частиною сучасного життя. Учасники соціальних мереж оприлюднюють особисту інформацію без жодних застережень. Так само можлива ймовірність навмисного або випадкового оприлюднення конфіденційної інформації підприємства, на якому працюють ці учасники. Із зростанням поширення інформації через соціальні мережі зростає інтерес до неї.

Метою роботи є дослідження існуючих методів виявлення агентів загроз конфіденційності та розширення досліджень із [3] на певну множину груп соціальної мережі з метою виявлення перехресних результатів щодо агентів та зведення їх у мережу агентів впливу.

## **Результати дослідження**

Кількісних показників виявлення агентів впливу порівняно мало. Більшість показників опирається на психологічні характеристики особистості, які можуть бути вдало приховані під час дослідження.

У [1] було проведено дослідження з використанням соціограм 11 людей, у якій кожному із досліджуваних пропонувалось представити себе в цій групі, визначити позицію і прогнозувати виконання запитів іншими людьми.

У [2] описано метод виявлення агентів загроз на основі модифікації соціометричних показників, що не потребує безпосереднього опитування потенційних агентів. Описаний метод є перспективним інструментом для виявлення агентів загроз конфіденційності серед агентів, що є складовою соціальної мережі. Групування кількісних значень коефіцієнтів дозволяє здійснити кількісний аналіз інформаційних процесів у соціальній мережі.

У [3] наведено результати дослідження неформальної комунікації у соціальних мережах для виявлення агентів загроз конфіденційності, а також описано розробку програмного забезпечення як інструменту досліджень, на прикладі конкретної соціальної групи розглянуто застосування програмного забезпечення.

Для проведення досліджень було розроблено програмне забезпечення на основі розробок [2] і [3]. Дане програмне забезпечення дозволяє розширити дослідження та виявити агентів загроз конфіденційності на множині груп соціальної мережі. Отримані показники дають уявлення про активність особистості у певній соціальній групі, показників його ставлення до групи та групи до нього. Порівняння цих показників відносно множини груп дають уявлення про можливу прихильність потенційного агента до активності у групах учасників підприємства-конкурента, що може свідчити про можливий витік інформації через даного співробітника.

## Висновки

Дослідження методів виявлення агентів загроз конфіденційності виявило, що найбільш поширеними є методи, які полягають в опитуванні потенційних агентів. Та існують і такі, що виключають цю необхідність. Наприклад, метод виявлення агентів загроз на основі модифікації соціометричних показників не потребує безпосереднього опитування потенційних агентів. Для проведення досліджень за даним методом було розроблене програмне забезпечення, що дозволяє виявити агентів загроз конфіденційності на множині груп соціальної мережі. Показники, що отримані в ході досліджень можуть бути використані підприємством для виявлення осіб, що можуть нести загрозу конфіденційності інформації.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Smith R.A. Understanding the Influential People and Social Structures Shaping Compliance / R.A. Smith, E.L. Fink // Journal of Social Structure. — 2015. — Vol. 16. — 15 і. — Режим доступу: <https://www.cmu.edu/joss/content/articles/volume16/SmithFink.pdf>
2. Нікіфорова Л. О. Метод розрахунку рівня вмотивованості співробітників щодо збереження конфіденційності інформації в задачах інформаційної безпеки / Л. О. Нікіфорова // Інформаційна безпека. — 2014. — № 4 (16). — С. 175-182.
3. Нікіфорова Л. О. Дослідження показників неформальної комунікації у соціальних мережах для виявлення агентів загроз конфіденційності / Л. О. Нікіфорова, Н. В. Горох, Г. О. Лебедева, О. В. Салієва // Реєстрація, зберігання і обробка даних. — 2016. — Т. 18, № 1. — С.52-62

**Чернецька Марія Вікторівна** — студентка групи 2УБ-13, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: mariachernetska@outlook.com

Науковий керівник: **Шиян Анатолій Антонович** — кандидат фізико-математичних наук, професор, Вінницький національний технічний університет, м. Вінниця

**Chernetska Mariia V.** — Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: mariachernetska@outlook.com

Supervisor: **Shyian Anatoliy A.** — PhD, Professor, Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia