

## КЛАСИФІКАЦІЯ ПРОФІЛІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АКТОРІВ СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСІВ

Соціальні інтернет-сервіси (СІС) представляють собою дієвий інструмент групової взаємодії учасників віртуальних спільнот, яких називають акторами [1–3]. В свою чергу, актори виступають джерелом контенту СІС, за допомогою якого інформують інших учасників віртуальних спільнот, виражають власну точку зору на актуальні події. Однак, такий контент може бути недостовірним, неповним або мати упереджений характер, створюючи передумови для поширення у суспільстві соціальної напруженості, протестних настроїв, маніпулювання суспільною думкою тощо. Тому СІС є ефективним засобом проведення інформаційних операцій проти людини, суспільства, держави [3].

При створенні профілів акторів СІС користувачі вводять персональну інформацію, сформульовану в анкеті. Тому використання узагальнених даних профіля актора, його публікацій у віртуальних спільнотах, особливості взаємодії з іншими акторами [3–5] є перспективним напрямком наукових досліджень для побудови їх профілів інформаційної безпеки. Під *профілем інформаційної безпеки актора СІС* будемо розуміти набір агрегованих характеристик профіля актора у СІС, які дозволяють визначити рівень його загрози як можливого учасника інформаційних акцій, направлених проти інформаційної безпеки людини, суспільства, держави [5]. Розробка методів автоматизованої побудови профілів інформаційної безпеки акторів і моделей прийняття рішень щодо їх залучення до інформаційних акцій є актуальним теоретико-прикладним завданням на шляху вирішення проблеми розроблення ефективної системи забезпечення інформаційної безпеки держави у СІС.

Аналіз останніх досліджень і публікацій [1–3] показав, що атрибути профілів акторів у СІС прийнято поділяти на числові – вік, рівень доходів та категоріальні – сімейний стан, професія, життєві цінності та інші, а набір конкретних значень атрибутів формує його загальну характеристику. У загальному випадку профіль актора у СІС містить в явному або прихованому вигляді інформацію, достатню для прийняття рішення щодо його залучення до інформаційних акцій. Таким чином, існує об'єктивне протиріччя між рівнем розвитку інформаційних технологій та науковим базисом автоматизованого виявлення загроз в СІС, а відсутність дієвих методик аналізу профілів акторів для раннього попередження інформаційних впливів додатково актуалізує обраний напрямок досліджень.

Розроблений спосіб побудови профілів безпеки акторів СІС [5] ґрунтується на класифікації за значеннями атрибутів, не суперечить науковим дослідженням М. Pennacchiotti та А.-М. Popescu [4] й зводиться до такого.

*Етап 1. Аналіз атрибутів профіля актора СІС.* Атрибути профіля актора СІС є опосередкованим джерелом інформації про його особу та інтереси. Суттєве значення для розв'язку задачі побудови профіля інформаційної безпеки

актора мають наступні його атрибути: ім'я актора; місця народження та проживання; навчальний заклад і місце роботи.

*Етап 2. Визначення показників активності публікації контенту.* Встановлено, що серед акторів СІС, залежно від особливостей публікації контенту, виділяють такі категорії: споживачі та постачальники. До першої з них відносяться актори, які нечасто публікують контент, мають велику кількість друзів і схильні до інформаційного пошуку, коментують публікації інших акторів й вступають з ними в діалог. Друга категорія акторів часто публікує власний контент або гіперпосилання на сторонні інформаційні ресурси у СІС. Таким чином, встановлення показників частоти публікації контенту різного походження, геш-тегів, гіперпосилань тощо, їх аналіз і узагальнення дозволяють віднести актора СІС до однієї з визначених категорій.

*Етап 3. Встановлення ознак, властивих контенту профіля актора.* Особливості мови актора, його життєві цінності, сфера інтересів проявляються вживанням відповідних лінгвістичних одиниць у текстових публікаціях. При цьому текстовий контент представляється у вигляді непов'язаного набору слів або *Bag of Words*.

*Етап 4. Аналіз зв'язків актора у СІС.* Інформативними атрибутами профіля актора у СІС є його зв'язки з іншими акторами і віртуальними спільнотами, згадування їх у дописах чи поширення контенту. Для аналізу зв'язків актора у СІС враховано такі атрибути його профіля: загальна кількість друзів, підписників і віртуальних спільнот актора; характеристика профілів друзів і віртуальних спільнот актора; поширення контенту друзів і віртуальних спільнот.

*Етап 5. Визначення класу загрози.* Після оцінки усіх характеристик профіля актора СІС необхідно віднести його до одного із заданих класів загроз. Для цього використано методи машинного навчання з учителем, а саме методи, які ґрунтуються на процедурах бустингу бінарних класифікаторів. Суть бустингу зводиться до побудови композиції алгоритмів машинного навчання, коли кожен наступний алгоритм компенсує недоліки композиції усіх попередніх алгоритмів.

Перевагою запропонованого підходу до класифікації профілів інформаційної безпеки акторів є врахування вартості помилок класифікації, що дозволяє реалізувати ефективний моніторинг інформаційного середовища СІС.

Запропонований у метод класифікації інформаційних профілів акторів СІС дозволяє автоматизувати процедури раннього виявлення загроз інформаційній безпеці держави. За даними побудованого профіля системою забезпечення інформаційної безпеки держави приймається щодо залучення акторів до інформаційних операцій у СІС. Розроблений метод відрізняється від відомих застосуванням сучасних методів інтелектуального аналізу даних, зокрема методів машинного навчання з учителем, і його узагальненням для використання у різних видах СІС. Таким чином, метод класифікації профілів інформаційної безпеки акторів підвищує ефективність і швидкодію системи забезпечення інформаційної безпеки держави у СІС.

### **Список використаних джерел:**

1. Панченко В. М. Соціальні інтернет-сервіси як засіб прихованого інформаційного впливу // *Інформаційна безпека людини, суспільства, держави.* – 2012. – № 1(8). – С. 65–69.
2. Грищук Р. В. *Основи кібернетичної безпеки : моногр.* / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.
3. Молодецька К. В. Узагальнена класифікація загроз інформаційній безпеці держави в соціальних інтернет-сервісах / К. В. Молодецька // *Защита информации : сб. науч. трудов.* – 2016. – Вып. 23. – С. 75–87.
4. Pennacchiotti M. *Democrats, republicans and Starbucks aficionados: user classification in Twitter* / M. Pennacchiotti, A. M. Popescu // *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining.* – ACM, 2011. – С. 430–438.
5. Молодецька-Гринчук К. В. *Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів* / К. В. Молодецька-Гринчук // *Інформаційна безпека.* – 2017. – № 2(26). – С. 104–110.