УДК 004.056:159.95

Л. О. Нікіфорова, Н. В. Горох, Г. О. Лєбєдєва, О. В. Салієва
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Дослідження показників неформальної комунікації у соціальних мережах для виявлення агентів загроз конфіденційності

Наведено результати дослідження неформальної комунікації у соціальних мережах для виявлення агентів загроз конфіденційності. Описано розроблену комп'ютерну програму як засіб для проведення дослідження, надано приклад застосування розробленого засобу для аналізування конкретної соціальної групи.

***Ключові слова**: агент, загроза конфіденційності, виявлення, соціальна мережа, неформальна комунікація.*

Вступ

У Стратегії кібербезпеки України зазначено: «Метою Стратегії кібербезпеки України (далі — Стратегія) є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави» [1]. Там же у п. 4.1 визначено: «Розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у: … створенні системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;…».

Таким чином, відповідно до Стратегії кібербезпеки України, до забезпечення інформаційної безпеки підприємства повинен залучатися широкий загал суб'єктів інформаційної безпеки. Це ж саме стверджується у сучасних стандартах інформаційної безпеки серії ISO/IEC 27000-27037 Information technology — Security techniques.

Дослідження кількісних значень показників неформальних комунікацій, які впливають на захист конфіденційності потрібен як для використання при розробці моделей і методів захисту інформації, так і для їхньої верифікації. Крім того, такі кількісні результати можуть бути використані як нормативні величини в умовах розробки та проектування систем захисту конфіденційності з урахуванням специфічних характеристик конкретного об'єкта захисту.

Таким чином, дослідження показників неформальної комунікації у соціальних мережах для виявлення агентів загроз конфіденційності є важливим напрям-

ком для наукових розробок, який часто може мати критично важливе значення для забезпечення інформаційної безпеки суб'єктів захисту.

Аналіз останніх досліджень і публікацій

Характеристики, які є перспективними для використання в дослідженнях неформальних комунікацій для виявлення агентів загроз, базуються, в основному, на менеджменті та управлінні персоналом [2–5]. На жаль, для них часто використовують методи психологічного чи соціологічного характеру, які потребують безпосереднього спілкування із суб'єктом загроз. Це призводить до підвищення ризику того, що такі характеристики не будуть виявлені внаслідок приховування інформації досліджуваним суб'єктом — агентом загроз конфіденційності.

Кількісних же показників, які є найбільш інформативними для розглядуваних задач, є не так вже багато. Серед них виділяються соціометричні показники, запропоновані Я. Морено наприкінці 1950-х років [6]. Проведені дослідження виявили, що ці показники можуть бути ефективно застосовані в умовах підприємств України [7]. Але принциповою вадою застосування існуючих інформаційних технологій [8, 9] є необхідність опитування агентів загроз, що унеможливлює як оперативне отримання необхідної інформації, так і скритий від агентів загроз її моніторинг. У [10] запропоновано метод узагальнення соціометричних показників із використанням соціальних мереж.

Сьогодні дослідження соціальних мереж зосереджені в основному на моделюванні агрегованих показників, які характеризують такі мережі [11]. При цьому агенти часто покладаються однаковими. Останнім часом, однак, зростає кількість досліджень, які направлені на виявлення впливових людей у соціальних мережах: ці результати є вкрай важливими для проблеми дифузії інновацій або виявлення агентів впливу. Наприклад, у [12] було використано в якості інструмента соціограми 11 людей, у якій кожному із 195-ти досліджуваних пропонувалося представити себе в цій групі, визначити позицію для себе, вибрати інший елемент для взаємодії, і прогнозувати їхню ймовірність виконання прохань іншого агента.

У [13] запропоновано метод визначення соціальної ролі агентів у соціальних мережах, який застосовано для мереж Facebook і Wikipedia. Цей метод базується на тому, що припускає існування ролей заздалегідь, що обмежує область застосування отриманих результатів.

У [14] розглянуто ряд моделей формування соціальних мереж, задачею яких є проілюструвати, як саме прагнення агентів до передачі інформації (тобто до становлення зв'язків з іншими агентами) сприяє їхній дифузії інформації по мережі. Основна увага дослідження була зосереджена щодо утворення циклічних структур із агентів у соціальній мережі.

Таким чином, існуючі методи та інструменти для їх реалізації не забезпечують повне та анонімне для агентів дослідження комунікації в соціальних мережах, що обмежує їхнє застосування до задачі виявлення агентів загроз конфіденційності та створення безпечного для людини та суспільства кіберпростору.

Метою статті є дослідження показників неформальної комунікації в соціальних мережах для виявлення агентів загроз конфіденційності, отриманих із ви-

користанням розробленого програмного забезпечення на основі метода, запропонованого в [10].

Метод виявлення агентів загроз

У роботі використано метод [10], так як він, на відміну від існуючих [6–9], не потребує здійснення опитування потенційних агентів загроз. Це дозволяє як уникнути інформування суб'єктів щодо включення їх у множину потенційних загроз конфіденційності, так і здійснювати моніторинг показників, які характеризують їхню потенційну небезпеку.

Коротко опишемо цей метод для випадку таких соціальних мереж, в яких використовуються тільки позитивні відгуки («лайки») одних агентів щодо інших. Метод може бути подано у такій формі.

Етап 1. Формується множина H співробітників, які потенційно можуть бути агентами загроз.

Етап 2. Для кожного i-го агента формується множина $R_{i\to j}$ лайків, які він надав кожному j-му агенту.

Етап 3. Для кожного i-го агента формується множина $R_{i\leftarrow jj}$ лайків, які він отримав від кожного j-го агента.

Етап 4. Для кожного i-го агента за формулою

$$P_{i\to} = \frac{1}{(N-1)} \sum_{j=1, j\neq i}^{N-1} R_{i\to j} \tag{1}$$

розраховується кількість лайків, якими цей агент відмітив пости всіх інших агентів впливу на підприємстві. Тут через N позначена загальна кількість агентів впливу.

Етап 5. Для кожного i-го агента за формулою

$$P_{i\leftarrow} = \frac{1}{(N-1)} \sum_{j=1, j\neq i}^{N-1} R_{i\leftarrow j} \tag{2}$$

розраховується кількість лайків, якими пости i-го агента відмітили всі інші агенти впливу.

Етап 6. Використовуючи формули (1) та (2) для кожного i-го агента впливу, розраховується «коефіцієнт взаємності» за такою формулою:

$$M_i = \frac{P_{i\leftarrow}}{P_{i\to}}. \tag{3}$$

Етап 7. Впорядковується значення M_i в порядку зменшення числових значень. Менші значення відповідають тому, що агент загроз намагається приймати участь у комунікативній діяльності групи, але група не сприймає його як «важливого» чи «значущого» для групи особи. Саме ці агенти загроз мають найменший рівень вмотивованості до збереження конфіденційності, постійно знаходячись в

умовах фактичної ізоляції від інших агентів. І саме тому вони, з часом, будуть найменше цінувати думку колективу. Тому ті агенти загроз, які знаходяться на початку, будуть утворювати загрозу конфіденційності інформації. Таким чином, на цьому етапі створюється рейтинг агентів, які вмотивовані утворювати загрози конфіденційності.

Етап 8. Виділяються 5–9 агентів, які мають найнижчі значення коефіцієнта взаємності (або 10 % агентів, коли кількість агентів загроз N є досить великою), які будуть складати множину T агентів загроз конфіденційності, щодо якої потрібно спільно структурам інформаційної безпеки та управління персоналом здійснити діяльність по збільшенню рівня адаптації до комунікації у колективі цих агентів загроз.

Для можливості використання даного методу для дослідження показників неформальної комунікації у соціальних мережах щодо виявлення агентів загроз конфіденційності необхідно розробити засіб (а саме — програмне забезпечення) для його реалізації.

Засіб для реалізації дослідження

Алгоритм для реалізації методу у вигляду комп'ютерної програми для соціальної мережі Вконтакте має наступний вигляд.

1. У програму додаються акаунти (використовуючи загальнодоступні ідентифікатори користувачів соціальної мережі Вконтакте).

2. Акаунти об'єднуються в групу, яка надалі буде досліджуватись.

3. Для кожного користувача групи через API-мережі завантажуються його особисті записи зі стіни.

4. Перевіряється останній запис зі стіни, який міститься в базі даних програми, зі списком, що отриманий від API.

5. Записи на стіні, які відсутні, додаються до загального списку.

6. Для кожного користувача групи через API-мережі завантажується інформація стосовно лайків на особистих записах (на основі даних про записи на стіні, що зібрані раніше).

7. Кожний запис аналізується: якщо зі списку користувачів, що поставили на цей запис лайк, присутні користувачі досліджуваної групи, інформація про поставлений лайк записується до бази даних.

8. Після зібрання всіх даних, при відображені групи дані по лайкам сортуються відповідно до заданого користувача.

9. Для кожного користувача за формулами (1) та (2) визначається коефіцієнт взаємності «Я до групи» та «Група до мене».

10. Для кожного користувача за формулою (3) визначається коефіцієнт взаємності.

11. Користувачі впорядковуються в порядку зменшення коефіцієнта взаємності.

Проект реалізовується, використовуючи мову програмування ASP.NET MVC із застосуванням специфічної форми інверсії управління (англ. — Inversion of control, IoC) — Dependency Injection, а саме її реалізації Ninject Framework. Роботу з базою даних забезпечує технологія Entity Framework. Для роботи з відкритим

API соціальної мережі впроваджено реалізацію відправки/отримання запитів від сервера. Для відображення графіків використовується бібліотека Chartjs. Авторизація користувачів виконується засобами OAuth Vkontakte.

UML-структуру залежності проектів для алгоритму подано на рис. 1.

Проект реалізації алгоритму складається із 9-ти підпроектів.

За відображення даних у браузері відповідає проект Sociality.Presentation, що складається із контролерів, де оброблюються дані для відображення, моделей даних та безпосередньо самого відображення.

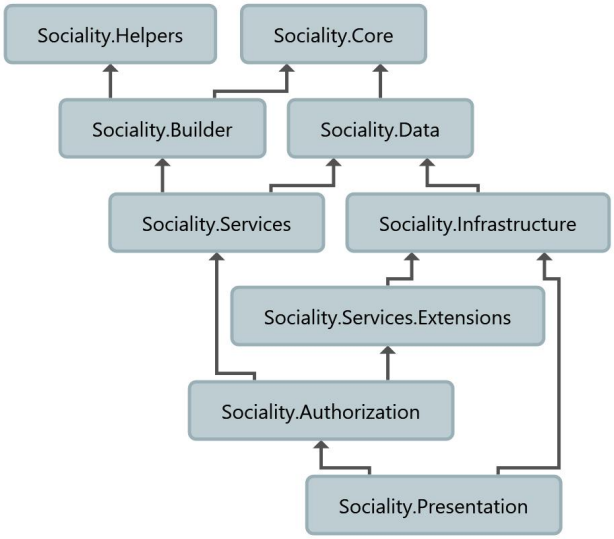

Рис. 1. UML-структура залежності проектів

Процес авторизації користувачів оброблюється у проекті Sociality.Authorization. Авторизація користувачів відбувається, використовуючи соціальну мережу Вконтакте, тому доступ до програми отримають лише користувачі, які зареєстровані у даній мережі.

Роботу із соціальною мережею забезпечує проект Sociality.Helpers: він реалізовує запити до API-мережі та обробляє відповіді (формат запитів — Json).

Для роботи з даними використовуються три проекти: Sociality.Core, Sociality.Data та Sociality.Services. У першому описуються всі реалізовані таблиці бази даних, що використовується програмою, у вигляді класів. Другий відповідає за підключення програми до бази даних, у ньому міститься опис усіх залежностей у таблицях, а також він відповідає за зміни у структурі бази, які можуть виникнути в процесі роботи (так звані міграції). Ну і в третьому проекті реалізовані загальні методи роботи з даними, такі як: отримати елемент таблиці по ідентифікатору, змінити чи видалити його і т.д.

Для відображення даних зазвичай використовуються додаткові моделі з цими даними, які формуються у класі Sociality.Builder. Так як проект побудовано засобами залежностей, для доступу усіх проектів до налаштувань цієї залежності вони були винесені у проект Sociality.Infrastructure, а у Sociality.Services.Extensions додатково винесені основні параметри роботи із сервісами.

UML-структуру зв’язку бази даних подано на рис. 2.

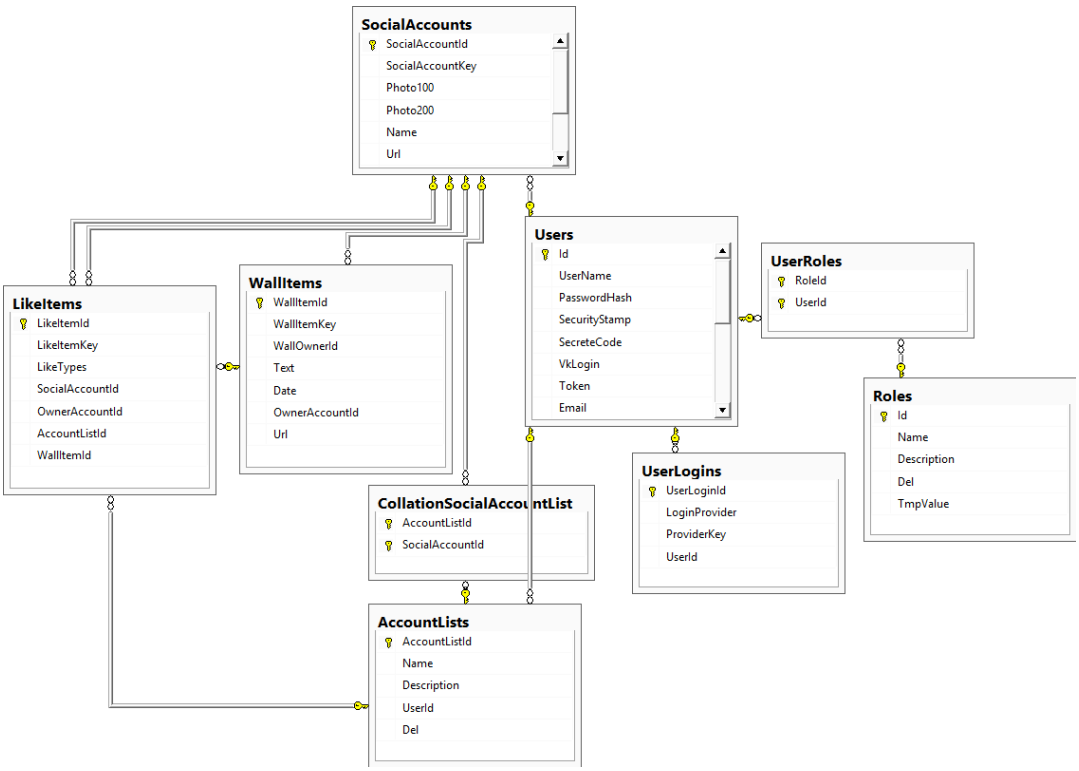

Рис. 2. UML-структура зв’язку таблиць бази даних

База даних проекту складається із 9-ти таблиць. Після успішної реєстрації, через механізм OAuth до програми надходять дані про користувача — його поштова адреса, ПІБ, нік, телефон і т.д. Ці дані записуються у таблицю Users. Для різних ролей користувачів у системі (наприклад, адміністратор, модератор, SEO-спеціаліст тощо) існує табличка Roles, а так як у користувача може бути декілька ролей одночасно, спроектовано табличку зв’язку UserRoles. Авторизацію реалізовано, використовуючи соціальну мережу Вконтакте, це фіксується у табличці UserLogins — з якої соціальної мережі користувач авторизувався.

Коли авторизований користувач додає до програми певні акаунти із мережі, використовуючи загальнодоступний нік, програма через API-мережі отримує дані щодо користувача та заносить їх у таблицю SocialAccounts.

Коли користувач об’єднує у групу, яка буде аналізуватися, акаунти, сформовані раніше (елементи таблиці SocialAccounts), створюється запис у таблицю AccountLists щодо створеної групи (її ім’я, короткий опис) та акаунти, які їй належать додаються у таблицю зв’язку акаунта з групою CollationSocialAccountList. Створюється окрема таблиця зв’язку між акаунтом та групою CollationSocialAccountList, так як слід передбачити, що один акаунт може належати до декількох груп.

Після створення групи дані стосовно записів на стіні соціальної мережі записуються/оновлюються у таблицю WallItems, а дані стосовно лайків, що отримані в мережі, — у таблицю LikeItems.

Результати дослідження

Головне меню авторизованого користувача подано на рис. 3. З його використанням користувач може створювати окремі групи, які складаються із різних агентів (тобто із різних акаунтів).

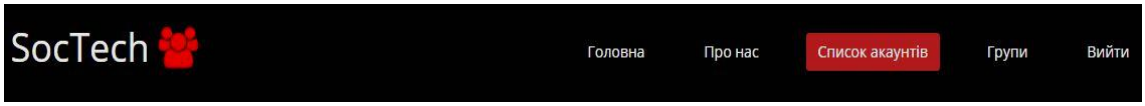

Рис. 3. Головне меню авторизованого користувача

Для дослідження було вибрано академічну групу студентів, яка налічувала $N = 26$ осіб. Всі студенти є учасниками соціальної мережі Вконтакте. З метою збереження персональних даних прізвища студентів упущені.

На рис. 4 подано розподіл кількості отриманих лайків для кожного агента із виділеної групи. Програма дозволяє також у окремому вікні подати розподіл кількості лайків, які поставив кожен із агентів даної групи іншим агентам.

На всіх рисунках і в таблиці, які наведено в статті, прізвища агентів закриті з метою збереження конфіденційності.

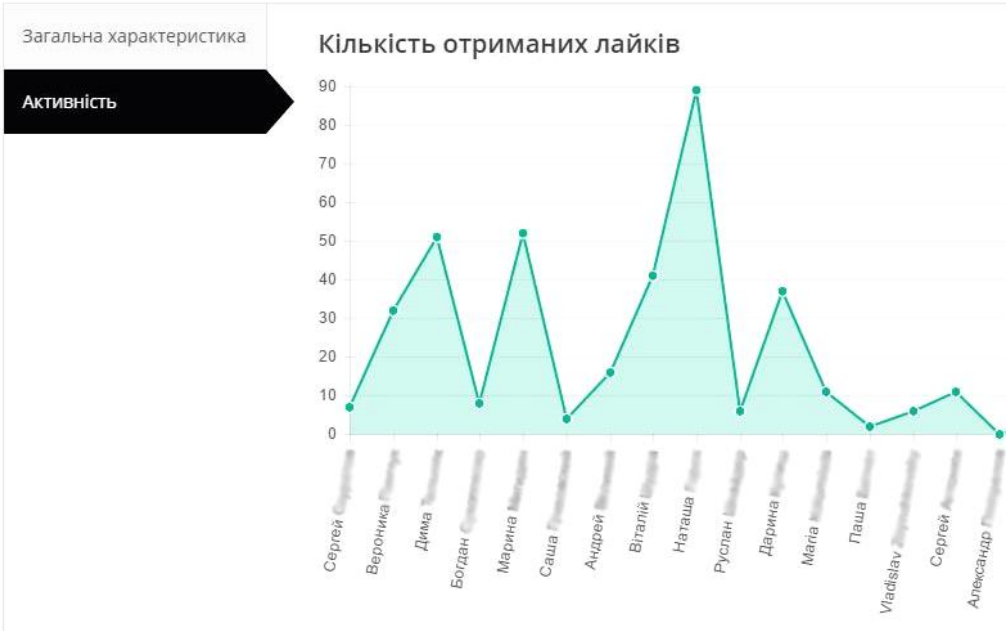

Рис. 4. Розподіл кількості отриманих лайків для кожного агента із виділеної групи

Як видно, у даній соціальній групі отримані лайки розподілені нерівномірно. Виділяється група суб'єктів, на яких група практично не звертає уваги. Також виділена група суб'єктів, які є у колі інтересів соціальної групи.

Програма дозволяє також представити результати у вигляді кругової діаграми (рис. 5), що збільшує наочність представлення матеріалів. На цій діаграмі подано розраховану за формулою (2) відносну кількість лайків, які соціальна група

надала до виділеного агента. Числові значення відповідного показника подано в таблиці.

Із рис. 5 видно, що до чотирьох агентів («Наташа», «Вероника», «Марина» та «Дима») даною соціальною групою приділяється велика увага, причому кількісні значення показника, які характеризують цю увагу, не сильно відрізняються (див. таблицю).

Для аналізу як отриманих, так і наданих кожним із агентів лайків, у комп'ютерній програмі здійснюються розрахунки за формулами (1), (2) та (3). Результати відповідних розрахунків подано на рис. 6, де наведено лише частину агентів.

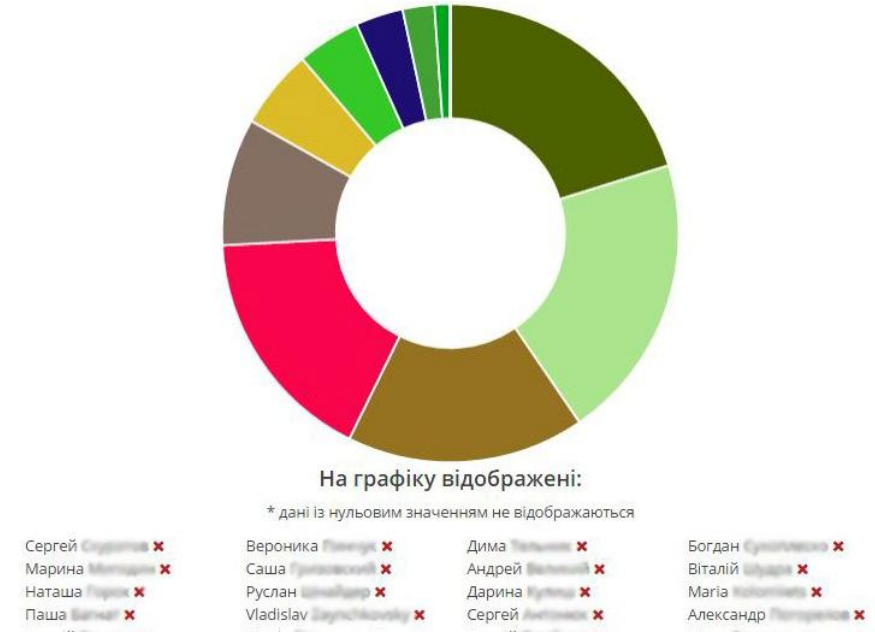

Рис. 5. Графічне відображення розподілу кількості лайків, якими соціальна група відмітила пости заданого агента

Коефіцієнт взаємності

* червоним кольором відмічені ті учасники групи, які не поставили та не отримали лайків

* жовтим кольором відмічені ті учасники групи, які поставили та не отримали лайків або навпаки

Акаунт	Група до акаунта	Акаунт до групи	Коефіцієнт
Иван	1,60 (40 likes)	0,08 (2 likes)	20,00
Андрій	1,12 (28 likes)	0,24 (6 likes)	4,67
Саша	0,16 (4 likes)	0,04 (1 likes)	4,00
Михаєль	0,12 (3 likes)	0,60 (15 likes)	0,20
Александр	0,00	0,00	--
Саша	0,00	0,00	--
Максим	0,00	0,24	--

Рис. 6. Результати розрахунку величин $R_{\leftarrow}$, $R_{\rightarrow}$ та M_i (наведено лише частину результатів, так як вони займають два вікна на екрані)

У таблиці подано всі розраховані комп'ютерною програмною результати для кількісних значень коефіцієнтів (1)–(3).

Результати розрахунків величин $R_{\leftarrow}$, $R_{\rightarrow}$ та M_i. Результати впорядковані за зменшення величини коефіцієнта взаємності M_i

№ за/п	Акаунт	Група до аканта $R_{\leftarrow}$	Акаунт до групи $R_{\rightarrow}$	Коефіцієнт M_i
1	Иван	1,60 (40 likes)	0,08 (2 likes)	20,00
2	Андрій	1,12 (28 likes)	0,24 (6 likes)	4,67
3	Саша	0,16 (4 likes)	0,04 (1 likes)	4,00
4	Дима	2,12 (53 likes)	0,64 (16 likes)	3,31
5	Наташа	3,64 (91 likes)	1,56 (39 likes)	2,33
6	Сергей	0,44 (11 likes)	0,20 (5 likes)	2,20
7	Андрій	0,16 (4 likes)	0,08 (2 likes)	2,00
8	Марія	1,40 (35 likes)	0,72 (18 likes)	1,94
9	Віталій	1,68 (42 likes)	1,08 (27 likes)	1,56
10	А Б	1,12 (28 likes)	0,76 (19 likes)	1,47
11	Женя	1,04 (26 likes)	0,88 (22 likes)	1,18
12	Сергей	0,32 (8 likes)	0,36 (9 likes)	0,89
13	Вероника	2,24 (56 likes)	2,56 (64 likes)	0,88
14	Богдан	0,72 (18 likes)	0,88 (22 likes)	0,82
15	Vladislav	0,32 (8 likes)	0,44 (11 likes)	0,73
16	Андрей	0,64 (16 likes)	1,00 (25 likes)	0,64
17	Марина	2,28 (57 likes)	4,20 (105 likes)	0,54
18	Maria	0,96 (24 likes)	2,04 (51 likes)	0,47
19	Дарина	1,48 (37 likes)	3,56 (89 likes)	0,42
20	Паша	0,08 (2 likes)	0,24 (6 likes)	0,33
21	Бодя	0,12 (3 likes)	0,40 (10 likes)	0,30
22	Руслан	0,40 (10 likes)	1,36 (34 likes)	0,29
23	Михаєль	0,12 (3 likes)	0,60 (15 likes)	0,20
24	Александр	0,00	0,00	–
25	Саша	0,00	0,00	–
26	Максим	0,00	0,24	–

Таким чином, для даної соціальної групи агентами загроз конфіденційності можуть бути «Михаєль», «Александр», «Саша» та «Максим».

Із представлених результатів можна зробити такі загальні висновки.

По-перше, понад половина досліджуваної соціальної групи, кількісні значення коефіцієнтів взаємності M_i яких переважають 0,7–0,8, досить комфортно відчувають себе у взаємодії з групою.

По-друге, виділяється відносно невелика підгрупа із восьми агентів, рівень активності яких у групі є досить великий (кількісні значення коефіцієнта $R_{\rightarrow}$ яких переважають усереднене по групі значення 1,00).

По-третє, виділяється підгрупа із 11-ти агентів, увага до яких у членів групи є переважаючою (кількісні значення коефіцієнта $R_{\leftarrow}$ яких переважають усереднене по групі значення 1,00). Як видно, група цікавиться діяльністю майже половини агентів зі свого складу.

По-четверте, виділяється підгрупа із двох агентів, які взагалі не взаємодіють із соціальною групою. Ці агенти можуть складати загрозу конфіденційності, так

як і вони не цінують своє спілкування із соціальною групою, і група не прагне спілкуватися з ними.

Обговорення та висновки

Розроблений у статті засіб (комп'ютерна програма) засвідчив свою перспективність використання як інструмент для виявлення агентів загроз конфіденційності.

На відміну від існуючих програмних продуктів [8, 9] і використаних у ряді досліджень [12] методик, запропонований в статті засіб не потребує безпосереднього спілкування з агентами. Це дозволяє використовувати його як інструмент для скритного аналізування ситуації у заданій соціальній групі. Особливо це важливо для задач забезпечення захисту конфіденційності, так як існуючі комп'ютерні засоби можуть, по-перше, налякати зловмисника та, по-друге, зловмисник, знаючи про проведення аналізу, може надавати викривлені дані.

У рамках запропонованої комп'ютерної програми є можливість виділити агентів впливу на соціальну мережу як осіб, які мають найвищі числові значення коефіцієнта $R_{\leftarrow}$. Це дозволяє застосувати цю програму до задач і проблем, які розглядались у статтях [12–14]. Унаслідок цього запропонована комп'ютерна програма може бути застосована до широкого кола задач як моделювання соціальних мереж [11, 14], так і для підвищення їхньої захищеності від витоку конфіденційної інформації.

Можна зробити такі висновки.

1. Запропонований засіб є перспективним інструментом для виявлення агентів загроз конфіденційності у випадку, коли агенти є складовою соціальної мережі.

2. Групування кількісних значень коефіцієнтів $R_{\leftarrow}$, $R_{\rightarrow}$ та M_i дозволяє здійснити аналіз інформаційних процесів у соціальній мережі, виявити неформальних агентів впливу на мережу та агентів, які ігноруються мережею, та тих агентів, які фактично ігнорують діяльність мережі (майже не приймаючи участь у її діяльності).

3. Запропонований засіб застосовується без участі агентів соціальної мережі, що виключає викривлення результатів дослідження, так як виключається канал неконтрольованого впливу на соціальну мережу. Це підвищує рівень вірогідності отриманих даних.

4. Запропонована комп'ютерна програма є потужним інструментом для здійснення моніторингу соціальних мереж, так як вона може використовуватися навіть у фоновому режимі. Це дозволяє отримати динаміку коефіцієнтів $R_{\leftarrow}$, $R_{\rightarrow}$ та M_i у її часовому розгортанні. Зокрема, це дозволяє вчасно виявити агентів, які стають потенційною загрозою конфіденційності.

1. *Стратегія* кібербезпеки України. Указ Президента України № 96/2016 від 15 березня 2016 року.

2. *Управління* персоналом / [Ожиганова М.І., Хорошко В.О., Яремчук Ю.Є., Карпінець В.В.]. — Вінниця: ВНТУ, 2014. — 188 с.

3. *Стратегія* управління інформаційною безпекою / [Андреєв В.І., Козюра В.Д., Скачек Л.М., Хорошко В.О.]. — К.: ДУІКТ, 2007. — 277 с.

4. *Основи* інформаційної безпеки / [Андреєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є.]. — К.: ДУІКТ, 2009. — 292 с.

5. *Богуш В.М.* Теоретичні основи захищених інформаційних технологій / В.М. Богуш, О.А. Довидьков, В.Г. Кривуца. — К.: ДУІКТ, 2010. — 454 с.

6. *Морено Я.Л.* Социометрия: Экспериментальный метод и наука об обществе / Я.Л. Морено. — М.: Академический Проект, 2001. — 384 с.

7. *Мороз О.В.* Соціально-психологічні чинники мотивування працівників приладобудівних підприємств / О.В. Мороз, Л.О. Нікіфорова, А.А. Шиян. — Вінниця: ВНТУ, 2011. — 252 с.

8. *Комп'ютерна* програма координатно-соціаграмного аналізу колективу Соціометрія. [Електроний ресурс]. — Режим доступу: http://www.ait.org.ua/socuometriya/

9. *Компьютерная* программа для автоматизации расчета данных социометрии SociometryPro [Электронный ресурс]. — Режим доступа: http://www.ledisgroup.com/ru/sociometryproru

10. *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.

11. *Jackson M.O.* Social and Economic Networks / M.O. Jackson. — Princeton: Princeton University Press, 2010. — 520 p.

12. *Smith R.A.* Understanding the Influential People and Social Structures Shaping Compliance [Електроний ресурс] / R.A. Smith, E.L. Fink // Journal of Social Structure. — 2015. — Vol. 16. — 15 p. — Режим доступу: https://www.cmu.edu/joss/content/articles/volume16/SmithFink.pdf

13. *Doran D.* On the discovery of social roles in large scale social systems / D. Doran // Social Network Analysis and Mining. — 2015. — Vol. 5. — Article 49. — 18 p.

14. *Prell Ch.* Network formation and knowledge gains / Ch. Prell, Lo. Yi-Jung // Journal of Mathematical Sociology. — 2016. — Vol. 40, Issue 1. — P. 21–52.

Надійшла до редакції 14.03.2016