УДК 004.056.5:004.942 DOI: 10.31673/2412-4338.2026.029103

Запорожченко Михайло Михайлович
доктор філософії, доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-0182-9497
m.zaporozhchenko@duikt.edu.ua

Легомінова Світлана Володимирівна
доктор економічних наук, професор, завідувач кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-4433-5123
s.legominova@duikt.edu.ua

Якименко Юрій Михайлович
кандидат військових наук, доцент, доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-6848-852X
y.yakymenko@duikt.edu.ua

Рабчун Дмитро Ігорович
кандидат технічних наук, доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-5555-0910
d.rabchun@duikt.edu.ua

ОЦІНЮВАННЯ ЙМОВІРНОСТІ ПОШИРЕННЯ СОЦІОІНЖЕНЕРНОЇ АТАКИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ З УРАХУВАННЯМ СПРЯМОВАНОСТІ КОМУНІКАЦІЙНОЇ ВЗАЄМОДІЇ

Анотація. *У статті розглянуто питання удосконалення підходу до оцінки поширення соціоінженерної атаки в корпоративній інформаційній системі шляхом урахування спрямованості комунікаційної взаємодії між користувачами. Актуальність дослідження зумовлена тим, що в задачах моделювання поширення соціоінженерного впливу успішність атаки визначається не лише характеристиками окремих користувачів, а й структурою зв'язків між ними. Особливе значення при цьому має комунікаційна складова. Метою статті є удосконалення підходу до оцінки поширення соціоінженерної атаки в корпоративній інформаційній системі шляхом урахування спрямованості комунікаційної взаємодії між користувачами та визначення впливу такого уточнення на результати оцінювання ймовірностей компрометації. У статті використано графове подання взаємодії між користувачами, ймовірнісне моделювання поширення атаки між пов'язаними вузлами та порівняльний аналіз результатів для симетричного й асиметричного варіантів графа за різних порогів відсікання траєкторій. Запропоновано декомпозицію сумарної інтенсивності комунікації між парою користувачів на дві напрямлені складові з використанням коефіцієнта спрямованості, що дозволило формалізувати нерівномірний розподіл комунікаційної активності між протилежними напрямами взаємодії. За результатами моделювання встановлено, що врахування спрямованості комунікаційної взаємодії приводить до зниження підсумкових оцінок імовірності компрометації порівняно із симетричним поданням графа та підвищує чутливість моделі до порога відсікання траєкторій. Показано, що асиметричне подання комунікаційної складової забезпечує більш вибіркове та структурно коректне відображення умов поширення соціоінженерної атаки. Практичне значення одержаних результатів полягає в можливості використання запропонованого підходу для оцінювання ймовірності поширення соціоінженерного впливу в корпоративних інформаційних системах.*

Ключові слова: *управління інформаційною безпекою, кібербезпека, соціоінженерна атака, корпоративна інформаційна система, графова модель, ймовірність компрометації.*

Mykhailo Zaporozhchenko
Ph.D., Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-0182-9497
m.zaporozhchenko@duikt.edu.ua

Svitlana Lehominova
Doctor of Sciences in Economics, Professor, Head of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-4433-5123
s.legominova@duikt.edu.ua

Yuriy Yakymenko
Candidate of Military Sciences, Associate Professor, Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-6848-852X
y.yakymenko@duikt.edu.ua

Dmytro Rabchun
Candidate of Technical Sciences
Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-5555-0910
d.rabchun@duikt.edu.ua

EVALUATION OF THE PROBABILITY OF SOCIAL ENGINEERING ATTACK PROPAGATION IN A CORPORATE INFORMATION SYSTEM WITH ACCOUNT FOR THE DIRECTIONALITY OF COMMUNICATION INTERACTION

Abstract. *This article addresses the improvement of an approach to evaluating the propagation of a social engineering attack in a corporate information system by accounting for the directionality of communication interaction between users. The relevance of the study stems from the fact that, in modeling the propagation of social engineering influence, attack success is determined not only by the characteristics of individual users, but also by the structure of the links between them. In this context, the communication component is of particular importance. The aim of the article is to improve the approach to evaluating the propagation of a social engineering attack in a corporate information system by accounting for the directionality of communication interaction between users and to determine the effect of this refinement on the estimated probabilities of compromise. The study employs a graph-based representation of user interaction, probabilistic modeling of attack propagation between connected nodes, and a comparative analysis of the results obtained for symmetric and asymmetric graph variants under different trajectory cutoff thresholds. A decomposition of the total communication intensity between a pair of users into two directed components using a directionality coefficient is proposed, which makes it possible to formalize the uneven distribution of communication activity across opposite directions of interaction. The modeling results demonstrate that accounting for the directionality of communication interaction leads to lower final estimates of compromise probability compared with the symmetric graph representation and increases the sensitivity of the model to the trajectory cutoff threshold. It is shown that an asymmetric representation of the communication component provides a more selective and structurally adequate description of the conditions under which a social engineering attack propagates. The practical significance of the obtained results lies in the possibility of applying the proposed approach to evaluate the probability of social engineering influence propagation in corporate information systems.*

Keywords: *information security management, cybersecurity, social engineering attack, corporate information system, graph model, compromise probability.*

1. Вступ

Соціоінженерні атаки залишаються одним із найбільш небезпечних типів загроз для корпоративних інформаційних систем, оскільки їх реалізація зумовлюється не лише технічними характеристиками середовища, а й особливостями поведінки користувачів, організацією службової взаємодії та характером внутрішнього інформаційного обміну. На відміну від суто технічних сценаріїв компрометації, у цьому випадку успішність атаки істотно залежить від людського чинника та умов взаємодії між учасниками корпоративного середовища. У корпоративних інформаційних системах соціоінженерний вплив доцільно розглядати не лише як одноразову дію, спрямовану на окремого користувача, а і як процес, що за певних умов може поширюватися через наявні міжкористувацькі зв'язки. Такий характер реалізації атаки ускладнює її оцінювання, оскільки потребує врахування не тільки властивостей окремого вузла, а й особливостей взаємодії в межах корпоративної структури.

За таких умов важливого значення набуває побудова підходів, що дозволяють оцінювати ймовірність реалізації соціоінженерної атаки з урахуванням міжкористувацьких зв'язків у корпоративній інформаційній системі. Це створює підґрунтя для точнішого аналізу умов компрометації та подальшого удосконалення моделей поширення соціоінженерного впливу.

2. Постановка проблеми

У задачах оцінювання поширення соціоінженерних атак у корпоративних інформаційних системах суттєве значення має адекватне подання міжкористувацької взаємодії, оскільки саме вона визначає умови переходу атаки між пов'язаними учасниками організаційного середовища. Особливу роль у цьому відіграє комунікаційна складова, через яку реалізуються повідомлення, запити, погодження та інші форми інформаційного обміну, потенційно релевантні для подальшого поширення соціоінженерного впливу.

Водночас у підходах до моделювання поширення атак комунікаційна взаємодія між користувачами часто подається в узагальненому вигляді, коли інтенсивність контактів в межах пари характеризується без явного розрізнення протилежних напрямів обміну. За такого подання однакова сумарна інтенсивність комунікації може

інтерпретуватися як однакові умови переходу атаки в обох напрямах, хоча в реальному корпоративному середовищі структура інформаційного обміну між користувачами нерідко є асиметричною.

Унаслідок цього різні за фактичною організацією комунікаційної взаємодії ситуації можуть отримувати однакові параметри зв'язку, що знижує чутливість моделей до реальної структури міжкористувацького обміну та може впливати на точність підсумкових оцінок поширення соціоінженерної атаки. Отже, актуальним є уточнення підходів до оцінювання поширення соціоінженерних атак шляхом урахування спрямованості комунікаційної взаємодії між користувачами.

3. Аналіз останніх досліджень і публікацій

У наявних публікаціях можна виокремити кілька основних напрямів. Частина робіт присвячена систематизації соціоінженерних атак, їх класифікації, типовим каналам реалізації та загальним сценаріям впливу [1-3]. Окремий блок досліджень орієнтований на оцінювання індивідуальної вразливості користувачів, профілювання потенційних жертв та кількісний аналіз ризику з урахуванням поведінкових і користувацьких характеристик [4-6]. Інший напрям охоплює графові, мережеві та стохастичні підходи, у межах яких соціоінженерна атака розглядається як процес поширення між пов'язаними вузлами, а взаємодія між користувачами подається через графи атак, багатошарові графові моделі або марковські процеси прийняття рішень [7-10]. Попри наявність таких досліджень, недостатньо деталізованим залишається питання подання саме спрямованості комунікаційної взаємодії між користувачами як окремого чинника оцінювання поширення соціоінженерної атаки. У більшості робіт увага зосереджена або на загальній структурі атак, або на індивідуальній вразливості користувача, або на мережевому поданні поширення загроз без спеціального акценту на асиметрії комунікаційного обміну в межах пари користувачів. Це зумовлює доцільність дослідження, спрямованого на врахування спрямованості комунікаційної взаємодії в задачі оцінювання поширення соціоінженерної атаки в корпоративній інформаційній системі.

4. Мета і задачі дослідження

Мета дослідження полягає в удосконаленні підходу до оцінювання ймовірності поширення соціоінженерної атаки в корпоративній інформаційній системі шляхом урахування спрямованості комунікаційної взаємодії між користувачами та визначення впливу такого уточнення на результати оцінювання ймовірностей компрометації.

Для досягнення мети визначено задачі дослідження, які мають бути досягнуті: аналіз обмежень симетричного подання комунікаційної взаємодії в задачі моделювання поширення соціоінженерної атаки; формалізація спрямованого подання комунікаційної складової для протилежних напрямів взаємодії в межах пари користувачів; визначення впливу урахування спрямованості комунікаційної взаємодії на результати оцінювання ймовірностей компрометації за симетричного та асиметричного подання графа.

5. Результати дослідження

У межах раніше запропонованого підходу [11] оцінювання ймовірності поширення соціоінженерної атаки в корпоративній інформаційній системі базується на аналізі взаємодії між користувачами, яка визначає можливість переходу атаки від одного вузла до іншого. Для опису такого переходу враховуються характеристики, що відображають спільну участь користувачів у проєктах, інтенсивність їх комунікаційної взаємодії, ієрархічну залежність, а також спільний доступ до інформаційних активів. Відповідні параметри задаються у вигляді інтенсивностей зв'язку, тоді як базові ймовірності переходу атаки за максимальної інтенсивності окремих типів взаємодії описуються параметрами p_{proj}, p_{com}, p_{hier} та p_{acc}. Надалі позначення виду (i,j) використовуються для характеристик, заданих для пари користувачів без урахування напряму, тоді як позначення виду $(i \to j)$ застосовуються для напрямлених характеристик взаємодії.

У зазначеній постановці проєктна взаємодія та спільний доступ до інформаційних активів подаються симетричними величинами $int_{proj}^{(i,j)}$ та $int_{acc}^{(i,j)}$, а ієрархічна залежність $int_{hier}^{(i\to j)}$ задається у напрямленому вигляді. Водночас комунікаційна складова подається узагальненою величиною $int_{com}^{(i,j)}$, спільною для обох напрямів взаємодії в межах однієї пари користувачів. Таке подання є прийнятним для загальної характеристики інтенсивності контактів, однак не дає змоги врахувати розподіл комунікаційної активності між напрямами $i \to j$ та $j \to i$.

Для задачі оцінювання ймовірності поширення соціоінженерної атаки таке спрощення є суттєвим обмеженням. Однакова сумарна інтенсивність комунікації не означає однакових умов поширення атаки в обох напрямах, оскільки в реальному корпоративному середовищі один із користувачів може значно частіше ініціювати повідомлення, узгодження або робочі запити, ніж інший. Унаслідок цього дві пари користувачів із різною структурою інформаційного обміну за симетричного подання комунікаційної складової можуть отримувати однакові оцінки ймовірності переходу атаки, хоча фактичні умови її поширення для них не є однаковими.

З метою усунення зазначеного обмеження пропонується перейти від симетричного подання комунікаційної взаємодії до її спрямованого опису. Для цього величина $int_{com}^{(i,j)}$, що характеризує інтенсивність комунікації між користувачами i та j, декомпонується на дві напрямлені складові:

$$int_{com}^{(i\to j)} = \alpha_{(i,j)} int_{com}^{(i,j)}, \quad (1)$$

$$int_{com}^{(j\to i)} = \left(1-\alpha_{(i,j)}\right) int_{com}^{(i,j)}, \quad (2)$$

де $\alpha_{(i,j)} \in [0;1]$ – коефіцієнт спрямованості комунікаційної взаємодії. Значення $\alpha_{(i,j)} = 0.5$ відповідає симетричному розподілу комунікаційної активності між двома напрямами, тоді як відхилення цього коефіцієнта від 0.5 відображає асиметрію комунікації в межах відповідної пари користувачів. Запропоноване подання зберігає сумарну інтенсивність комунікаційної взаємодії, проте змінює її розподіл між протилежними напрямами, що дає змогу точніше врахувати структуру інформаційного обміну між користувачами.

З урахуванням запропонованого уточнення ймовірність переходу атаки від користувача i до користувача j визначається за виразом:

$$P_{(i\to j)} = 1-\left(1-p_{proj}\right)^{int_{proj}^{(i,j)}}\left(1-p_{com}\right)^{int_{com}^{(i\to j)}}\left(1-p_{hier}\right)^{int_{hier}^{(i\to j)}}\left(1-p_{acc}\right)^{int_{acc}^{(i,j)}}. \quad (3)$$

Наведений вираз відрізняється від базової постановки лише способом подання комунікаційної складової, що дає змогу зберегти загальну логіку моделі та її сумісність із раніше визначеними проєктними, ієрархічними й ресурсними характеристиками зв'язку між користувачами. Ймовірність переходу атаки у зворотному напрямі $j \to i$ визначається аналогічно з урахуванням відповідної напрямленої інтенсивності комунікації та значення ієрархічної складової для цього напряму.

Визначення коефіцієнта $\alpha_{(i,j)}$ може здійснюватися як на основі фактичних даних, так і сценарно. За наявності інформації про кількість комунікаційних ініціацій у кожному напрямі доцільно використовувати співвідношення:

$$\alpha_{(i,j)} = \frac{n_{(i\to j)}}{n_{(i\to j)} + n_{(j\to i)}}, \quad (4)$$

де $n_{(i\to j)}$ є кількістю ініційованих контактів від користувача i до користувача j, а $n_{(j\to i)}$ – аналогічним показником у зворотному напрямі. За відсутності детальних статистичних даних значення $\alpha_{(i,j)}$ може задаватися в межах наперед визначених інтервалів відповідно до сценаріїв комунікаційної взаємодії.

Урахування спрямованості комунікаційної складової дає змогу перейти від агрегованого опису пари користувачів до диференційованого подання умов переходу атаки в кожному з двох протилежних напрямів. Якщо у симетричній постановці комунікаційний внесок у розрахунок визначається лише сумарною інтенсивністю контактів, то в уточненій постановці додатково враховується розподіл цієї інтенсивності між напрямами взаємодії. У результаті формуються різні значення ймовірностей $P_{(i\to j)}$ та $P_{(j\to i)}$, які точніше відображають фактичну структуру комунікаційного обміну.

Отримані значення напрямлених імовірностей переходу атаки використовуються як ваги дуг графа взаємодії користувачів корпоративної інформаційної системи. У такому поданні симетричний варіант моделі відповідає випадку рівномірного розподілу комунікаційної складової між протилежними напрямами, тоді як асиметричний варіант враховує її нерівномірний розподіл на основі коефіцієнта $\alpha_{(i,j)}$. Таким чином, запропоноване уточнення не змінює загальної архітектури підходу до моделювання поширення соціоінженерної атаки в корпоративній інформаційній системі, але забезпечує більш коректне подання комунікаційної складової як напрямленого фактора впливу. Це створює підстави для подальшого порівняльного аналізу результатів, отриманих за симетричного та асиметричного опису взаємодії між користувачами.

Для оцінювання впливу спрямованості комунікаційної взаємодії на результати моделювання багатоетапної соціоінженерної атаки було виконано порівняльний аналіз симетричного та асиметричного варіантів графа взаємодії користувачів. Розрахунки здійснювалися для двох значень порога відсікання траєкторій, що дало змогу оцінити не лише вплив спрямованості комунікаційної складової, а й чутливість підсумкових оцінок до зміни умов відбору траєкторій поширення атаки. Така постановка узгоджується з попередньо введеним поданням напрямлених імовірностей поширення атаки як ваг ребер графа взаємодії.

Узагальнені результати оцінювання ймовірностей компрометації для різних варіантів моделі наведено на рис. 1. Теплова карта показує, що симетричне подання графа в усіх розглянутих випадках формує вищі оцінки ймовірності компрометації, ніж асиметричне. Це означає, що рівномірний розподіл комунікаційної активності між протилежними напрямами призводить до більш інтенсивного поширення атаки в моделі, тоді як урахування її фактичної спрямованості знижує підсумкові оцінки. Такий результат є закономірним, оскільки в асиметричному поданні частина переходів отримує менші ваги порівняно із симетричною постановкою, а отже, їх внесок у загальне поширення атаки зменшується.

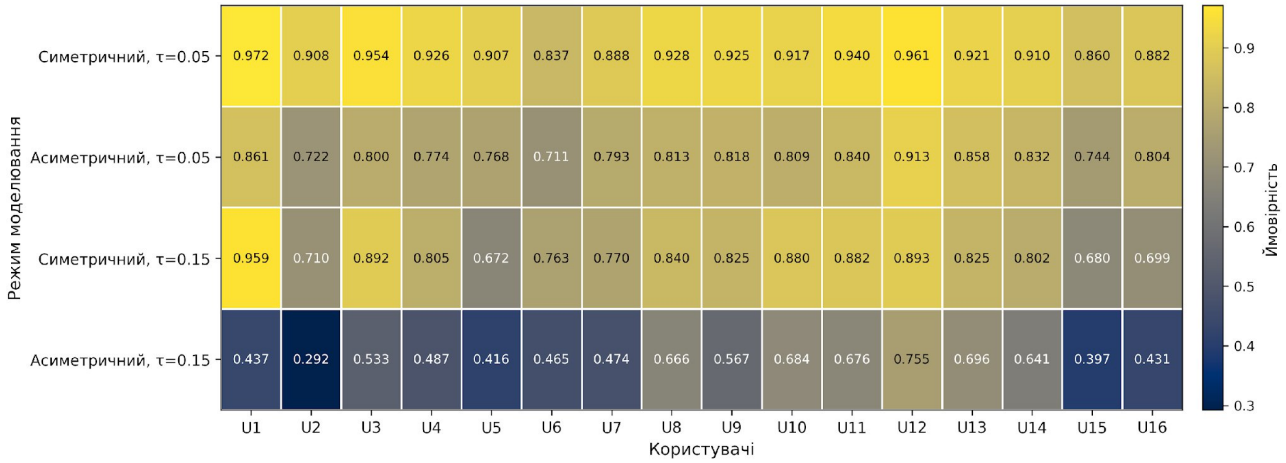

Рис. 1. Теплова карта ймовірностей компрометації для симетричного та асиметричного варіантів графа за різних значень порога відсікання траєкторій

Порівняння результатів за різних значень порога показує, що його підвищення зменшує оцінки ймовірності компрометації в обох варіантах моделі, однак ступінь цього зменшення є неоднаковим. Як видно з рис. 2 (ліва частина), в асиметричному графі зниження виражене суттєвіше, ніж у симетричному. Це свідчить про вищу чутливість асиметричної моделі до посилення порогового відсікання траєкторій. За врахування спрямованості комунікаційної взаємодії слабші маршрути поширення атаки швидше втрачають вплив, тоді як у симетричній моделі їх сумарний внесок залишається більшим.

Окремий інтерес становить порівняння симетричної та асиметричної моделей за фіксованих значень порога. Як показано на рис. 2 (права частина), різниця між ними зростає за жорсткішого відсікання траєкторій. Це означає, що за більш вибіркового врахування траєкторій поширення атаки вплив спрямованості комунікаційної складової проявляється сильніше. Інакше кажучи, коли модель зосереджується переважно на більш значущих траєкторіях, відмінність між рівномірним і нерівномірним розподілом комунікаційної активності стає більш вираженою.

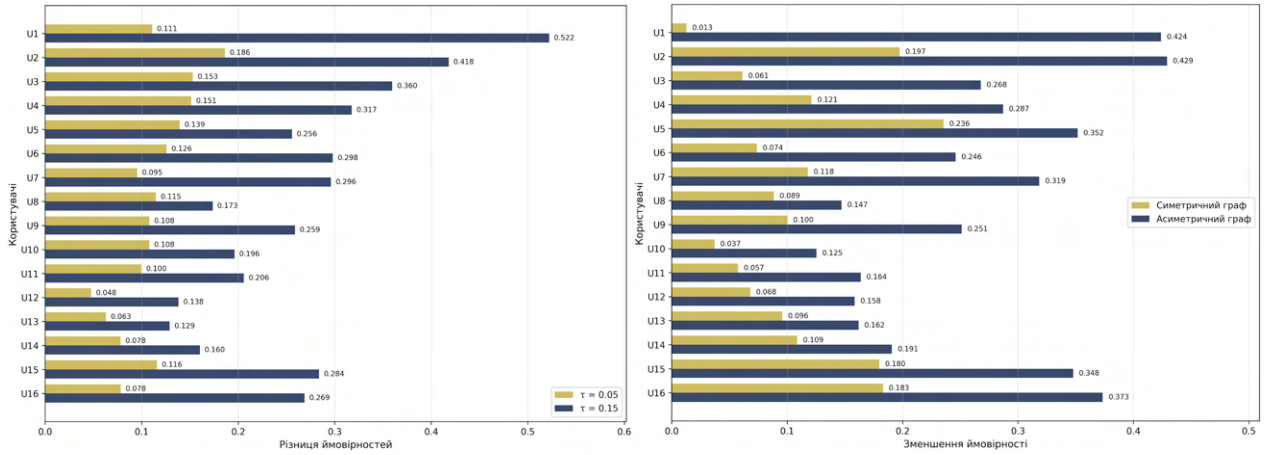

Рис. 2. Порівняльний аналіз змін ймовірності компрометації за різних умов моделювання: ліворуч – зміна оцінок при підвищенні порога відсікання траєкторій; праворуч – різниця між симетричною та асиметричною моделями за фіксованих значень порога

Виявлені кількісні закономірності підтверджуються також структурою самих графів взаємодії, наведених на рис. 3 та рис. 4 (для користувача $User_5$). На рис. 3 подано фрагмент графа взаємодії за нижчого порога відсікання траєкторій. У симетричному варіанті зв'язки між вузлами мають більш однорідний характер, що забезпечує збереження більшої кількості потенційних траєкторій атаки. В асиметричному варіанті ваги дуг розподіляються нерівномірно, унаслідок чого частина напрямів послаблюється, а структура можливого поширення стає більш вибірковою.

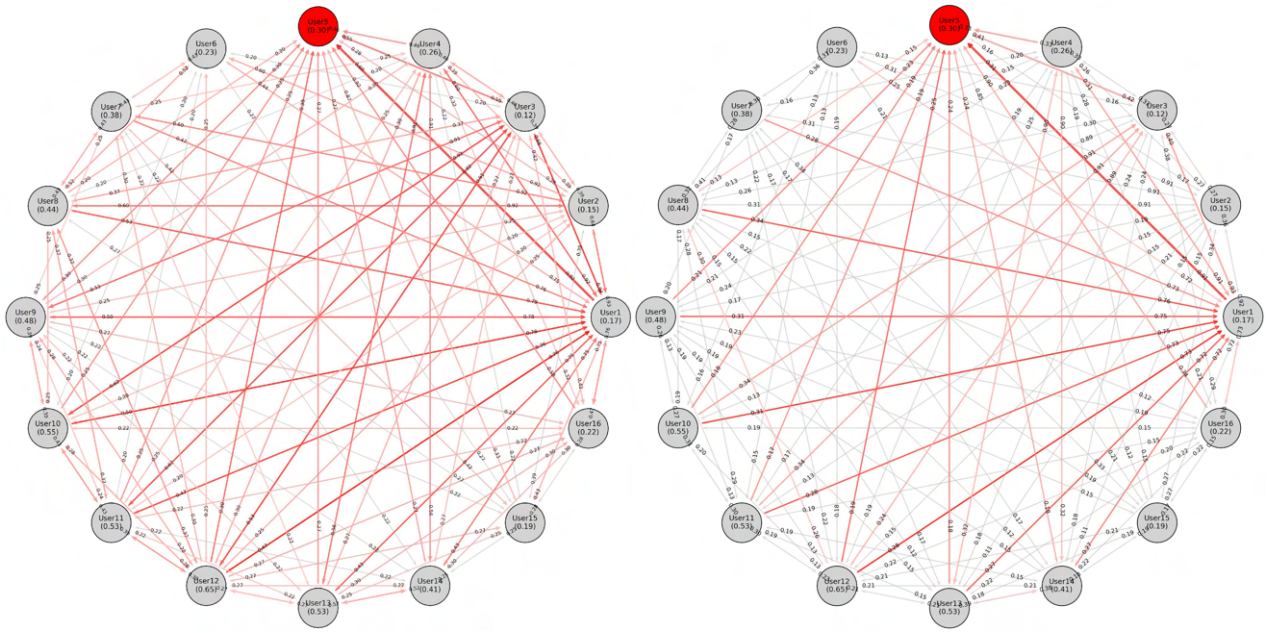

Рис. 3. Фрагмент графа взаємодії користувачів за порога відсікання траєкторій 0.05: ліворуч – симетричний варіант; праворуч – асиметричний варіант

На рис. 4 аналогічне порівняння наведено для вищого порога відсікання траєкторій. У цьому випадку ефект асиметрії проявляється ще виразніше: слабші напрямлені зв'язки швидше виключаються з подальшого розгляду, а кількість траєкторій, що зберігають суттєвий вплив на підсумкову оцінку компрометації, помітно скорочується. Саме тому різниця між симетричною та асиметричною моделями за жорсткішого порогового відсікання стає більш відчутною не лише кількісно, а й структурно на рівні графового подання.

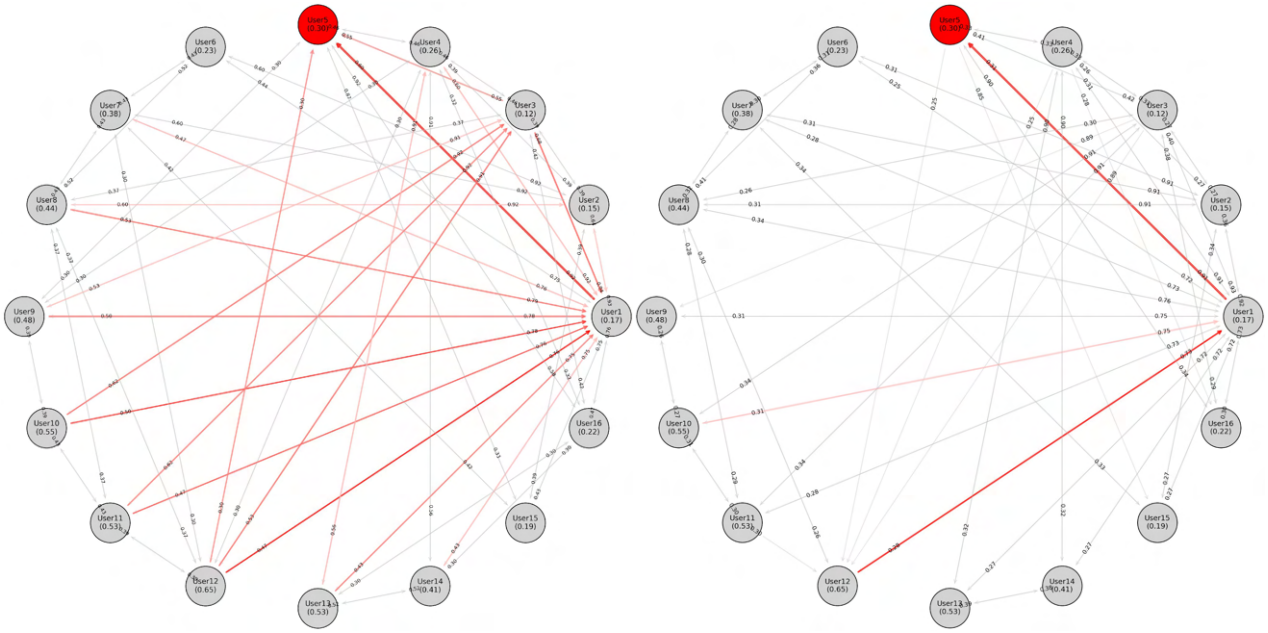

Рис. 4. Фрагмент графа взаємодії користувачів за порога відсікання траєкторій 0.15: ліворуч – симетричний варіант; праворуч – асиметричний варіант

Отже, результати моделювання підтверджують, що врахування спрямованості комунікаційної взаємодії змінює оцінки поширення соціоінженерної атаки не лише на рівні окремого переходу між користувачами, а й на рівні інтегральної оцінки компрометації у графі взаємодії. Асиметричне подання комунікаційної складової приводить до нижчих значень імовірності компрометації та виявляє вищу чутливість до порога відсікання траєкторій. Це дає підстави розглядати спрямовану модель комунікаційної взаємодії як більш точний інструмент опису умов поширення соціоінженерної атаки в корпоративній інформаційній системі.

6. Висновки та перспективи подальших досліджень

У статті удосконалено підхід до оцінки поширення соціоінженерної атаки в корпоративній інформаційній системі шляхом урахування спрямованості комунікаційної взаємодії між користувачами. На відміну від симетричного подання комунікаційної складової, запропонований підхід передбачає її декомпозицію на два протилежні напрями в межах пари користувачів із використанням коефіцієнта спрямованості, що дало змогу формалізувати нерівномірний розподіл комунікаційної активності між вузлами графа взаємодії.

У результаті проведеного моделювання встановлено, що врахування спрямованості комунікаційної взаємодії впливає не лише на локальні значення ймовірностей переходу атаки між користувачами, а й на підсумкові оцінки ймовірностей компрометації в межах графової моделі. Показано, що асиметричне подання графа систематично формує нижчі оцінки порівняно із симетричним, що свідчить про більш стримане та структурно вибіркове поширення атаки за умови врахування фактичного розподілу комунікаційних зв'язків.

Одержані результати також підтвердили, що асиметрична модель є більш чутливою до зміни порога відсікання траєкторій. За жорсткішого відбору маршрутів різниця між симетричним і асиметричним поданням посилюється, що вказує на зростання ролі спрямованості комунікації в умовах, коли в розрахунку враховуються переважно найбільш значущі траєкторії поширення атаки. Отже, запропоноване уточнення дозволяє підвищити точність оцінювання умов поширення соціоінженерної атаки в корпоративній інформаційній системі без зміни загальної архітектури базової моделі.

Перспективою подальших досліджень є розширення підходу в напрямі оцінювання спрямованості інших типів міжкористувацької взаємодії, а також апробація моделі на емпіричних даних корпоративних комунікаційних середовищ для уточнення правил параметризації коефіцієнта спрямованості та перевірки стійкості отриманих закономірностей.

Внесок авторів. Михайло Запорожченко – концептуалізація дослідження, методика, формалізація моделі, програмна реалізація та візуалізація результатів; Світлана Легомінова – наукове консультування, участь у формуванні методичних положень, інтерпретація результатів, критичний перегляд і редагування статті; Юрій Якименко – аналіз джерел, підготовка теоретичного підґрунтя дослідження; Дмитро Рабчун – перевірка коректності результатів моделювання та участь у формуванні висновків.

Декларація про штучний інтелект

Автор не використовував штучний інтелект при створенні матеріалів статті.

Конфлікт інтересів

Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social Engineering Attacks During the COVID-19 Pandemic. *SN Computer Science*, 2(2). https://doi.org/10.1007/s42979-020-00443-1

2. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, 198, 656–661. https://doi.org/10.1016/j.procs.2021.12.302

3. Rathod, T., Jadav, N. K., Tanwar, S., Alabdulatif, A., Garg, D., & Singh, A. (2025). A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing & Management*, 62(1), 103928. https://doi.org/10.1016/j.ipm.2024.103928

4. Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, 3(1). https://doi.org/10.1186/s42400-020-00047-5

5. Ye, Z., Guo, Y., Ju, A., Wei, F., Zhang, R., & Ma, J. (2020). A Risk Analysis Framework for Social Engineering Attack Based on User Profiling. *Journal of Organizational and End User Computing*, 32(3), 37–49. https://doi.org/10.4018/joeuc.2020070104

6. Benavides-Astudillo, E., Silva-Ordoñez, L., Rocohano-Rámos, R., Fuertes, W., Fernández-Peña, F., Sanchez-Gordon, S., & Bastidas-Chalan, R. (2022). Analysis of Vulnerabilities Associated with Social Engineering Attacks Based on User Behavior. In *Communications in Computer and Information Science* (pp. 351–364). Springer International Publishing. https://doi.org/10.1007/978-3-031-03884-6_26

7. Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. *Cybersecurity*, 4(1). https://doi.org/10.1186/s42400-021-00094-6

8. Zhou, P., Gu, X., Nepal, S., & Zhou, J. (2021). Modeling social worm propagation for advanced persistent threats. *Computers & Security*, 108, 102321. https://doi.org/10.1016/j.cose.2021.102321

9. Abri, F., Zheng, J., Namin, A. S., & Jones, K. S. (2022). Markov Decision Process for Modeling Social Engineering Attacks and Finding Optimal Attack Strategies. *IEEE Access*, 1. https://doi.org/10.1109/access.2022.3213711

10. Aijaz, M., & Nazir, M. (2023). Modelling and analysis of social engineering threats using the attack tree and the Markov model. *International Journal of Information Technology*. https://doi.org/10.1007/s41870-023-01540-z

11. Запорожченко М.М. (2024). Метод оцінки ймовірності реалізації траєкторій соціоінженерної атаки в корпоративних інформаційних системах. *Наукові записки Державного університету інформаційно-комунікаційних технологій*, 2. С. 236–242. https://doi.org/10.31673/2786-8362.2024.024719

References

1. Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social Engineering Attacks During the COVID-19 Pandemic. *SN Computer Science*, 2(2). https://doi.org/10.1007/s42979-020-00443-1

2. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, 198, 656–661. https://doi.org/10.1016/j.procs.2021.12.302

3. Rathod, T., Jadav, N. K., Tanwar, S., Alabdulatif, A., Garg, D., & Singh, A. (2025). A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing & Management*, 62(1), 103928. https://doi.org/10.1016/j.ipm.2024.103928

4. Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, 3(1). https://doi.org/10.1186/s42400-020-00047-5

5. Ye, Z., Guo, Y., Ju, A., Wei, F., Zhang, R., & Ma, J. (2020). A Risk Analysis Framework for Social Engineering Attack Based on User Profiling. *Journal of Organizational and End User Computing*, 32(3), 37–49. https://doi.org/10.4018/joeuc.2020070104

6. Benavides-Astudillo, E., Silva-Ordoñez, L., Rocohano-Rámos, R., Fuertes, W., Fernández-Peña, F., Sanchez-Gordon, S., & Bastidas-Chalan, R. (2022). Analysis of Vulnerabilities Associated with Social Engineering Attacks Based on User Behavior. In *Communications in Computer and Information Science* (pp. 351–364). Springer International Publishing. https://doi.org/10.1007/978-3-031-03884-6_26

7. Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. *Cybersecurity*, 4(1). https://doi.org/10.1186/s42400-021-00094-6

8. Zhou, P., Gu, X., Nepal, S., & Zhou, J. (2021). Modeling social worm propagation for advanced persistent threats. *Computers & Security*, 108, 102321. https://doi.org/10.1016/j.cose.2021.102321

9. Abri, F., Zheng, J., Namin, A. S., & Jones, K. S. (2022). Markov Decision Process for Modeling Social Engineering Attacks and Finding Optimal Attack Strategies. *IEEE Access*, 1. https://doi.org/10.1109/access.2022.3213711

10. Aijaz, M., & Nazir, M. (2023). Modelling and analysis of social engineering threats using the attack tree and the Markov model. *International Journal of Information Technology*. https://doi.org/10.1007/s41870-023-01540-z

11. Zaporozhchenko, M. (2024). A method for evaluating the probability of realization of social engineering attack trajectories in corporate information systems. *Scientific Notes of the State University of Information and Communication Technology*, 2, 236–242. https://doi.org/10.31673/2786-8362.2024.024719

Надійшла до редакції: 20.01.26
Прийнята до друку:12.06.26
Опубліковано:30.06.26