УДК 004.5:519.8 DOI: 10.31673/2786-8362.2024.024719

Запорожченко М.М.

МЕТОД ОЦІНКИ ЙМОВІРНОСТІ РЕАЛІЗАЦІЇ ТРАЄКТОРІЙ СОЦІОІНЖЕНЕРНОЇ АТАКИ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Zaporozhchenko M.M. A method for evaluating the probability of realization of social engineering attack trajectories in corporate information systems.

The article presents a method for assessing the probability of realization of trajectories of multi-stage social engineering attacks (SEA) in corporate information systems (CIS). The developed approach is based on mathematical modeling of interactions between users, which is a key factor in the spread of attacks in the corporate environment. The study takes into account four main criteria: joint projects, communications, hierarchical relationships, and shared access to information assets.

The proposed mathematical model allows to quantify the probability of an attack passing between pairs of users using indicators of the intensity of their interaction. The graph of user interaction built on the basis of the calculated probabilities reflects the potential trajectories of SEA spread in the CIS, allowing to identify the most critical links and key nodes of the system, through which the probability of compromise is highest.

The model is oriented and adapted to the specifics of the corporate environment, where attacks spread through trust, work, and hierarchical interactions. The application of the method makes it possible to identify vulnerable segments of the system, optimize response strategies, and develop preventive measures aimed to minimize the likelihood of a successful SEA.

Keywords: social engineering, graph model, risk assessment, attack probability, information security

Запорожченко М.М. Метод оцінки ймовірності реалізації траєкторій соціоінженерної атаки в корпоративних інформаційних системах.

У статті запропоновано метод оцінки ймовірності реалізації траєкторій багатоетапних соціоінженерних атак (SEA) у корпоративних інформаційних системах (КІС). Метод базується на математичному моделюванні взаємодій між користувачами з урахуванням спільних проєктів, комунікацій, ієрархічних зв'язків та спільного доступу до активів.

Розроблена модель дозволяє кількісно оцінити ймовірність поширення атак та побудувати граф взаємодій для виявлення найбільш критичних зв'язків і вузлів системи. Застосування методу допомагає визначати вразливі сегменти КІС, оптимізувати заходи реагування та мінімізувати ризики успішної реалізації SEA.

Ключові слова: соціальна інженерія, графова модель, оцінка ризиків, ймовірність атаки, інформаційна безпека

Вступ

Соціоінженерні атаки (SEA) залишаються критичною загрозою для корпоративних інформаційних систем (КІС), особливо їх багатоетапний варіант, що передбачає послідовну компрометацію користувачів через ланцюгові взаємодії в межах організаційних структур. На відміну від одноетапних атак, які обмежуються конкретною ціллю, багатоетапні SEA характеризуються поширенням загрози через проміжні ланки – скомпрометованих користувачів, що ускладнює своєчасне виявлення атаки та вимагає кількісної оцінки ймовірності переходів між етапами компрометації. Тому *актуальним* вважається завдання математичного моделювання та оцінки ймовірності реалізації траєкторій поширення SEA в корпоративному середовищі.

Аналіз останніх досліджень. Більшість сучасних підходів до оцінки захищеності користувачів і систем від SEA зосереджуються на одноетапних атаках, де основним об'єктом аналізу є індивідуальна вразливість користувача. У таких дослідженнях враховуються психологічні, поведінкові фактори, рівень обізнаності, компетентність у розпізнаванні загроз, а також організаційні та технічні заходи безпеки. Зокрема, у роботах [1,2] авторами запропоновано моделі для оцінки індивідуальної ймовірності компрометації користувача у соціальних мережах на основі сукупності зазначених факторів. Однак ці моделі не враховують взаємодію між користувачами, яка є критичним чинником у багатоетапних SEA.

У роботі [3] запропоновано метод інтеграції SEA у графи атак, що дозволяє об'єднати соціальні та технічні вразливості для комплексного аналізу загроз. Перевагою є використання кількісного аналізу графів, що сприяє формуванню всебічної стратегії захисту та є перспективним для моделювання багатоетапних атак. Недоліком є відсутність аналізу внутрішніх взаємодій користувачів у КІС, що обмежує застосування для оцінки ланцюгової компрометації.

У роботі [4] запропоновано фреймворк для оцінки вразливості користувачів до SEA у соціальних мережах, що поєднує соціально-психологічні, поведінкові та емоційні фактори. Перевагою є інтеграція різних характеристик користувача для формування єдиного профілю вразливості. Однак фреймворк орієнтований лише на соціальні мережі та не враховує взаємодії між користувачами як шляхи поширенні багатоетапних атаки.

Таким чином, недоліком більшості існуючих підходів є те, що вони не враховують динаміку корпоративних взаємодій, які формують потенційні траєкторії поширення SEA. Тому існує потреба у нових підходах, які враховують як індивідуальні фактори захищеності користувачів, так і інтенсивність їх взаємодії у корпоративному середовищі. Розробка моделей для оцінки ймовірності поширення SEA дозволить аналізувати не лише ймовірність успішної атаки на конкретного користувача, але й ризики ланцюгової компрометації, що виникають через робочі та довірчі відносини.

Метою роботи є розробка методу оцінки ймовірності реалізації траєкторій багатоетапних SEA у КІС. Основними завданнями є:

- визначення ключових факторів, що впливають на ймовірність переходу SEA від скомпрометованого користувача до іншого співробітника;
- побудова математичної моделі для оцінки ймовірності поширення SEA між парами користувачів;
- побудова математичної моделі для оцінки ймовірності реалізації траєкторій багатоетапної SEA.

Очікувані результати дослідження включають кількісну оцінку ймовірностей реалізації багатоетапних SEA, ідентифікацію слабких місць КІС та визначення найбільш вразливих сегментів для спрямування превентивних заходів безпеки.

Виклад основного матеріалу дослідження.

Успішність одноетапних (прямих) SEA визначається індивідуальними та організаційними факторами захищеності користувача, тоді як ймовірність поширення багатоетапних атак обумовлена структурними особливостями КІС, зокрема інтенсивністю комунікацій між користувачами та їхніми ролями в організаційній ієрархії.

Моделювання поширення багатоетапних атак фокусується виключно на інтенсивності взаємодії між користувачами, що пояснюється принциповою відмінністю між зовнішньою атакою та атакою, яка поширюється через скомпрометованого користувача. У другому випадку бар'єр для успішної реалізації атаки є значно нижчим, оскільки зловмисник отримує низку переваг [5,6]:

- імітація стилю комунікації – доступ до історії взаємодій і внутрішньої інформації дозволяє відтворити характерні мовні особливості, структуру повідомлень та типовий графік комунікації, що мінімізує підозри у отримувача повідомлення;
- довіра до джерела – використання легітимного корпоративного облікового запису або поштової адреси скомпрометованого користувача забезпечує високий рівень довіри до шкідливого контенту, значно підвищуючи ймовірність успішної взаємодії;
- знання корпоративного контексту – доступ до внутрішньої інформації (організаційна структура, активні проєкти, персональні дані співробітників) дозволяє точно адаптувати атаку до специфіки цільового користувача чи групи.

Застосування технічних засобів захисту в умовах багатоетапних атак також є обмеженим: антивірусні рішення, фільтри електронної пошти та системи моніторингу часто не здатні виявити загрози, що поширюються через легітимні корпоративні канали зв'язку. Крім того, внутрішні засоби комунікації організації, як правило, не піддаються повноцінному

моніторингу або фільтрації внутрішнього трафіку, що дозволяє атаці залишатися непоміченою на етапах її поширення.

Таким чином, інтенсивність комунікацій між користувачами виступає ключовим фактором поширення багатоетапних SEA, обумовлюючи необхідність кількісного аналізу цих взаємодій для оцінки ймовірності подальшої компрометації користувачів КІС.

Для оцінки ймовірності поширення атаки між користувачами КІС запропоновано використовувати такі критерії: спільні проєкти, комунікації, ієрархічні зв'язки між користувачами, спільний доступ до інформаційних активів.

Оцінка інтенсивності критерію **«спільні проєкти»** враховує рівень співпраці між користувачами як показник їхньої взаємодії. Висока частота спільної участі у проєктах може сприяти зміцненню робочих зв'язків і вказувати на залежність у робочих процесах, підвищуючи ризик поширення SEA через цю залежність. Етапи оцінки критерію «спільні проєкти» включають такі:

- визначення періоду спостереження (6-12 місяців), включно з коротко- та довгостроковими проєктами;
- збір даних про кількість спільних проєктів та ролі користувачів із корпоративних систем управління проєктами (Asana, Jira, Trello);
- нормалізація кількості спільних проєктів для пари користувачів за формулою: $int_{proj}^{i,j} = \frac{Project_{ij}}{Project_{max}}$, де $Project_{ij}$ – кількість спільних проєктів між користувачами i та j, $Project_{max}$ – максимальне значення кількості спільних проєктів серед всіх пар користувачів; $int_{proj}^{i,j} \in [0; 1]$, де 0 – відсутність співпраці, 1 – максимальний рівень співпраці; $i \neq j$.

Нормалізація усуває вплив абсолютних значень, що змінюються залежно від організації чи періоду аналізу.

Критерій **«комунікації»** включений до аналізу через сприяння частих контактів підвищенню довіри та накопиченню спільного контексту: інформації про робочі звички, очікуваних відповідей та типових запитів, що спрощує реалізацію атак [7]. Оцінка інтенсивності критерію «комунікації» здійснюється аналогічно попередньому:

- визначення періоду збору даних (1-6 місяців) для забезпечення репрезентативності;
- збір даних з корпоративних платформ комунікації (Microsoft Teams, Slack, Gmail, Zoom);
- нормалізація в межах $[0; 1]$ за формулою: $int_{com}^{i,j} = \frac{Com_{ij}}{Com_{max}}$.

Аналіз фокусується на інтенсивності зв'язків без розкриття змісту комунікацій, що забезпечує конфіденційність аналізу.

Критерій **«ієрархічні зв'язки»** між користувачами КІС впливає на ймовірність поширення SEA у випадках прямого підпорядкування («керівник-підлеглий»), сприяючи виконанню нетипових вказівок [8]. Етапи оцінки інтенсивності критерію «ієрархічні зв'язки» включають такі:

- збір даних з HRM-систем, що зберігають інформацію про організаційну структуру;
- розрахунок індикаторів: $int_{hier}^{i,j} = 1$, якщо користувач i є керівником користувача j; $int_{hier}^{i,j} = 0$, якщо прямого підпорядкування немає.

Критерій **«спільний доступ до активів»** (файлів, баз даних, систем) включений до аналізу на основі гіпотези, що користувачі зі спільним доступом до конфіденційних ресурсів мають підвищений рівень взаємодії та відповідальності, що може бути використано зловмисниками для подальшої компрометації системи через скомпрометованого користувача [9]. Етапи оцінки інтенсивності критерію «спільний доступ до активів» включають такі:

- збір інформації про права доступу користувачів з корпоративних IAM-систем;
- нормалізація в межах $[0; 1]$ за формулою: $int_{acc}^{i,j} = \frac{Access_{ij}}{Access_{max}}$.

Таким чином, визначені ключові фактори, що впливають на ймовірність переходу SEA від скомпрометованого користувача до іншого співробітника.

Наступним завданням була побудова математичної моделі для оцінки ймовірності поширення SEA між парами користувачів. Запропонована модель ґрунтується на гіпотезі, що збільшення кількості типів та інтенсивності взаємодій між користувачами підвищує кількість потенційних шляхів переходу атаки, а отже, ймовірність її успішного поширення [10]. Формально ймовірність непоширення атаки між парою користувачів визначається за формулою:

$$Q_{i,j} = \prod_{k=1}^{n} (1 - p_k)^{int_k^{i,j}}, \quad (1)$$

де p_k – ймовірність успішного поширення атаки в межах k-го типу взаємодії за максимальної інтенсивності ($int_k^{i,j} = 1$); $int_k^{i,j}$ – оцінка інтенсивності k-го типу взаємодії між користувачами (i, j).

Відповідно, оцінка ймовірності поширення атаки, визначається як доповнення до ймовірності непоширення, з урахуванням інтенсивності різних типів взаємодії:

$$P_{i,j} = 1 - \prod_{k \in \{proj,com,hier,acc\}} (1 - p_k)^{int_k^{(i,j)}}. \quad (2)$$

Для прикладного застосування методу базові ймовірності компрометації для кожного типу взаємодії визначено на основі типових корпоративних умов та обґрунтованих припущень щодо соціальних і організаційних зв'язків. Значення ймовірностей відображають різний ступінь ризику поширення SEA залежно від інтенсивності та природи взаємодії:

- **критерій «спільні проєкти»**: базове значення $p_{proj} = 0.4$ обґрунтоване помірною ймовірністю компрометації внаслідок професійної співпраці. Спільна участь у проєктах сприяє обміну робочою інформацією та формуванню певного рівня довіри, проте цей зв'язок зазвичай обмежується формальним робочим контекстом, що знижує ризик несанкціонованого впливу;
- **критерій «комунікації»**: базове значення $p_{com} = 0.6$ враховує, що частота комунікацій корелює з формуванням довірчих стосунків між користувачами. Регулярний обмін повідомленнями або іншими формами взаємодії створює основу для маніпуляцій, оскільки користувачі можуть менш критично оцінювати інформацію, отриману з довіреного джерела;
- **критерій «ієрархічні зв'язки»**: базове значення $p_{hier} = 0.9$ відображає високий рівень ризику компрометації через значний вплив керівників на підлеглих. Ієрархічні зв'язки часто супроводжуються довірою та зобов'язанням виконання інструкцій, що значно знижує бар'єр для поширення атаки;
- **критерій «спільний доступ до активів»**: базове значення $p_{acc} = 0.2$ обґрунтоване тим, що взаємозалежність у цьому випадку ґрунтується переважно на політиках доступу, а соціальні та комунікаційні зв'язки відсутні або є мінімальними, однак у разі компрометації спільного активу, що є критичним для робочих процесів, виникає опосередкована взаємодія між користувачами, яка може слугувати додатковим вектором поширення атаки.

Запропоновані значення ймовірностей є базовими і можуть бути скориговані на основі емпіричних даних, специфіки корпоративного середовища або експертних оцінок. Їх вибір забезпечує об'єктивну основу для моделювання ризиків та дозволяє адаптувати модель до умов конкретної організації.

В якості ілюстративного прикладу запропоновано такі значення інтенсивності взаємодії для певної пари користувачів: $int_{proj} = 0.6, int_{com} = 0.5, int_{hier} = 0, int_{acc} = 0.4$. Ймовірність переходу SEA може бути розрахована за формулою (2):

$$P_{i,j} = 1 - \left(1 - p_{proj}\right)^{int_{proj}^{i,j}} (1 - p_{com})^{int_{com}^{i,j}} (1 - p_{hier})^{int_{hier}^{i,j}} (1 - p_{acc})^{int_{acc}^{i,j}} =$$
$$= 1 - (1 - 0.4)^{0.6} (1 - 0.6)^{0.5} (1 - 0.9)^{0} (1 - 0.2)^{0.4} \approx 0.574.$$

У випадку наявності ієрархічного зв'язку (користувач i підлеглий користувача j) буде виконуватися нерівність $P_{j,i} > P_{i,j}$:

$$P_{j,i} = 1 - (1 - 0.4)^{0.6} (1 - 0.6)^{0.5} (1 - 0.9)^{1} (1 - 0.2)^{0.4} \approx 0.957.$$

Таким чином, побудовано математичну модель оцінки ймовірності поширення SEA між парами користувачів, що базується на кількісній оцінці інтенсивності взаємодії за визначеними факторами.

Наступним завданням була побудова математичної моделі для оцінки ймовірності реалізації траєкторій багатоетапної SEA. Для візуалізації траєкторій SEA було побудовано орієнтований (оскільки напрямок взаємодії впливає на ймовірність поширення атаки) зважений граф взаємодії співробітників КІС, в якому ребра позначають зв'язки між користувачами та відповідну ймовірність поширення атаки між ними, розраховану за формулою (2), а вузли графа позначають користувачів КІС і відповідну ймовірність успішної зовнішньої атаки з урахуванням факторів профілю захищеності (психологічного, організаційного, технічного факторів та фактору інформаційного впливу) (рис. 1).

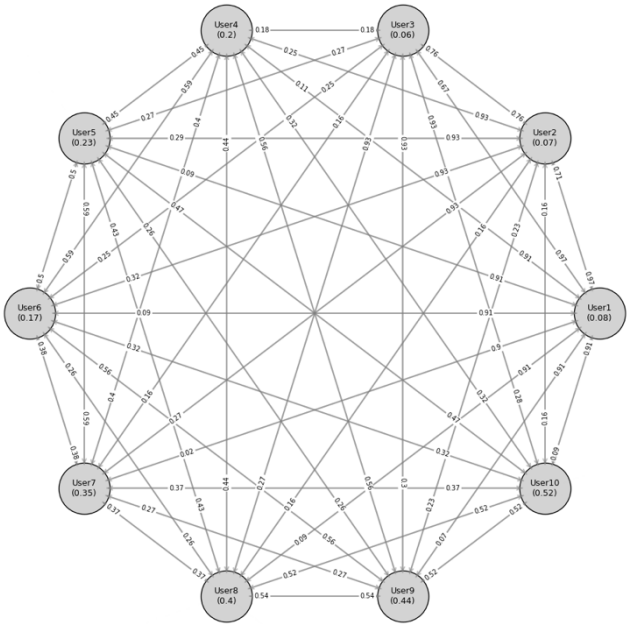

Рис. 1. Повний граф взаємодії користувачів

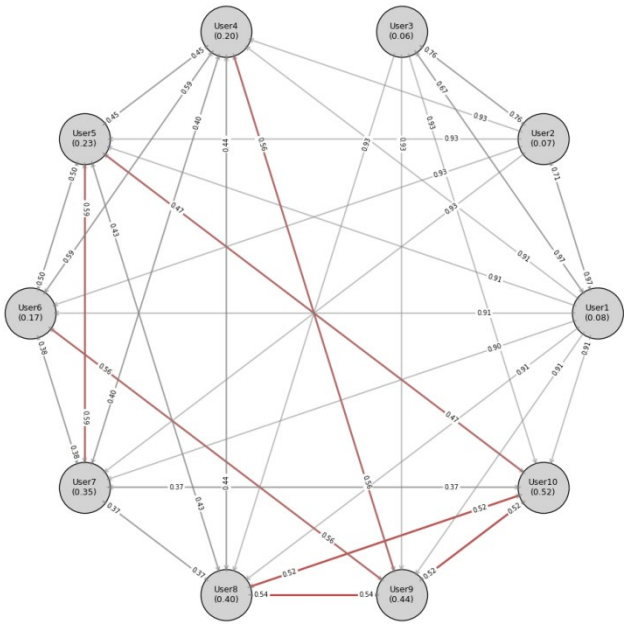

Рис. 2. Критичні траєкторії поширення соціоінженерної атаки ($p_T \geq 0.2$)

Для оцінки ймовірності реалізації траєкторії атаки її можна представити як впорядковану послідовність користувачів $(U_{k_1}, U_{k_2}, \dots, U_{k_{m-1}}, U_{k_m})$, де U_{k_1} – початковий скомпрометований користувач (внаслідок зовнішньої атаки), U_{k_m} – кінцевий користувач, $U_{k_2}, \dots, U_{k_{m-1}}$ – проміжні користувачі, через яких передається атака. Ймовірність успішної реалізації траєкторії SEA розраховується за формулою:

$$P_T = P_{k_1} \cdot \prod_{i=1}^{m-1} P_{k_i,k_{i+1}}, \tag{3}$$

де P_{k_1} – ймовірність успішної атаки на початкового користувача; $P_{k_i,k_{i+1}}$ – ймовірність переходу атаки від користувача U_{k_i} до наступного користувача в траєкторії $U_{k_{i+1}}$.

Запропонована модель розраховує ймовірність реалізації багатоетапної SEA шляхом поетапного аналізу переходів між користувачами. Це дозволяє виявити вразливі траєкторії SEA та ідентифікувати критичні переходи, що становлять найбільший ризик для КІС.

На основі повного графа (рис. 1) було здійснено пошук найбільш ймовірних траєкторій поширення SEA із використанням формули (3). Ідентифіковано ключових користувачів та зв'язки між ними, через які ймовірність поширення атаки є максимальною.

Скорочений граф траєкторій (рис. 2) побудовано шляхом виключення ребер з ймовірністю переходу менше 0.35 та траєкторій із загальною ймовірністю не більше 0.2. Це дозволяє зменшити обчислювальну складність моделі та сфокусувати аналіз на найбільш ризикованих шляхах поширення атаки. У результаті граф відображає критичні траєкторії, що забезпечує

ідентифікацію вразливостей КІС та пріоритизацію заходів захисту: $P(U_{10} \to U_8) = 0.2704$; $P(U_{10} \to U_9) = 0.2704$; $P(U_9 \to U_4) = 0.2464$; $P(U_9 \to U_6) = 0.2464$; $P(U_{10} \to U_5) = 0.2444$; $P(U_9 \to U_8) = 0.2376$; $P(U_9 \to U_{10}) = 0.2288$; $P(U_8 \to U_{10}) = 0.208$; $P(U_7 \to U_5) = 0.2065$.

При цьому ймовірність окремих багатоетапних атак виявляється більшою за ймовірність прямої атаки на окремих користувачів, наприклад, $P(U_9 \to U_4) > P(U_4), P(U_{10} \to U_5) > P(U_5), P(U_9 \to U_6) > P(U_6)$. Це пояснюється тим, що при багатоетапній атаці зловмисник отримує додаткові переваги, такі як накопичення знань про цільову систему, доступ до більшого обсягу конфіденційної інформації, а також можливість використання легітимних каналів комунікації, які підвищують довіру до атакуючих повідомлень. Крім того, компрометація проміжних вузлів забезпечує більшу адаптивність зловмисника до змін у системі захисту, що дозволяє йому ефективніше обходити існуючі механізми безпеки та збільшує шанси на успішну атаку на кінцевого користувача. Цей ефект є особливо помітним у корпоративних середовищах із високою інтенсивністю взаємодій між користувачами та складними організаційними зв'язками, де багатоетапна стратегія атаки стає більш вигідною та ефективною.

Таким чином, побудована математична модель для оцінки ймовірності реалізації траєкторій багатоетапної SEA, яка включає ймовірність прямої атаки на користувача, що розраховується на основі профілю його захищеності, та ймовірності поширення SEA між парами користувачів, що базується на кількісній оцінці інтенсивності взаємодії.

Висновки

У статті запропоновано метод оцінки ймовірності реалізації траєкторій багатоетапних SEA у КІС, що охоплює математичне моделювання та аналіз траєкторій SEA. Основні результати дослідження включають наступні:

- визначено ключові фактори, що впливають на ймовірність передачі атаки між користувачами, зокрема: спільні проєкти, комунікації, ієрархічні зв'язки та спільний доступ до інформаційних активів. Запропоновано критерії для кількісної оцінки інтенсивності взаємодії, що дозволяють формалізувати процес поширення атак у корпоративному середовищі;
- побудовано математичну модель для оцінки ймовірності передачі атак між парами користувачів. Модель враховує інтенсивність зв'язків та особливості корпоративної взаємодії, що дозволяє відстежувати динаміку поширення атак та визначати фактори, які посилюють їх ймовірність;
- розроблено підхід до аналізу траєкторій поширення SEA на основі орієнтованого зваженого графа взаємодій користувачів. Запропонована модель дозволяє ідентифікувати найбільш вразливі траєкторії атаки, визначити критичні переходи, що мають максимальний ризик для КІС, та оптимізувати граф шляхом виключення малоймовірних зв'язків для зниження обчислювальної складності.

Запропонований метод забезпечує кількісну оцінку ймовірностей реалізації багатоетапних SEA, дозволяючи виявляти слабкі місця системи та пріоритизувати превентивні заходи для їх нейтралізації. Практична реалізація результатів дослідження сприяє оптимізації управління ризиками та підвищенню рівня захисту корпоративних ІС шляхом фокусування зусиль на найбільш критичних сегментах системи.

Перспективи подальших досліджень включають розширення моделі для врахування асиметричних критеріїв взаємодії, що відображають напрямок комунікацій та рольову структуру користувачів, а також інтеграцію технологій штучного інтелекту для автоматизації аналізу та прогнозування траєкторій атак у динамічних умовах корпоративного середовища.

Список використаної літератури:

1. Albladi S., Weir G.R.S. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity.* 2020. Vol. 3. 7. URL: https://doi.org/10.1186/s42400-020-00047-5

2. Albladi S., Weir G.R.S. A conceptual model to predict social engineering victims. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. London, UK. 2019. P. 212-212. URL: https://doi.org/10.1109/ICGS3.2019.8688352

3. Beckers K., Krautsevich L., Yautsiukhin A. Using Attack Graphs to Analyze Social Engineering Threats. *International Journal of Secure Software Engineering (IJSSE).* 2015. Vol. 6, № 2. P. 47-69. URL: https://doi.org/10.4018/IJSSE.2015040103

4. Albladi S., Weir G.R.S. User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences.* 2018. Vol 8, № 1. 5. URL: https://doi.org/10.1186/s13673-018-0128-7

5. Khan N., Houghton R. J., Sharples S. Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks. *Cognition Technology and Work*. 2022. Vol. 24, № 3. P. 393-421. URL: https://doi.org/10.1007/s10111-021-00690-z

6. Haber, M.J. Insider and external threats. *Privileged Attack Vectors*. 2020. Apress, Berkeley, CA. P. 117-125. URL: https://doi.org/10.1007/978-1-4842-5914-6_7

7. Zeffane R., Tipu S., Ryan J. Communication, commitment & trust: exploring the triad. *International Journal of Business and Management.* 2011. Vol. 6, № 6. P. 77-87. URL: https://doi.org/10.5539/ijbm.v6n6p77

8. Suman S., Srivastava, A. K. Antecedents of organisational commitment across hierarchical levels. *Psychology and Developing Societies.* 2012. Vol. 24, № 1. P. 61-83. URL: https://doi.org/10.1177/097133361102400103

9. Halima Kure, Shareeful Islam. Assets focus risk management framework for critical infrastructure cyber security risk management. *IET Cyber-Physical Systems: Theory & Applications.* 2019. Vol. 4, № 4. P. 332-340. URL: https://doi.org/10.1049/iet-cps.2018.5079

10. Klünder J., Schneider K., Kortum F., Straube J., Handke L., Kauffeld S. Communication in teams – an expression of social conflicts. *6th International Conference on Human-Centred Software Engineering (HCSE) / 8th International Conference on Human Error, Safety, and System Development (HESSD).* Stockholm, Sweden. August 29-31, 2016. P. 111-129, URL: https://doi.org/10.1007/978-3-319-44902-9_8

Автор статті

Запорожченко Михайло – аспірант, старший викладач, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0003-0182-9497

Author of the article

Zaporozhchenko Mykhailo – postgraduate, senior lecturer, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0000-0003-0182-9497