## INFORMATION WARFARE

DOI 10.20535/2411-1031.2020.8.1.218001
УДК 004.056.53::519.171

РОСТИСЛАВ ГЕРАСИМОВ,
ОЛЬГА КРУК,
ОКСАНА ЦУРКАН,
ВАДИМ ЯШЕНКОВ

# МЕТОД АНАЛІЗУВАННЯ УРАЗЛИВОСТЕЙ СОЦІОТЕХНІЧНИХ СИСТЕМ ДО ВПЛИВІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Досліджено вплив соціальної інженерії на користувачів соціотехнічних систем. Для запобігання такому впливові запропоновано аналізування їх уразливостей стосовно форм маніпулювання свідомістю. З огляду на це виокремлено та зіставлено типові підходи до протидії використанню соціальної інженерії. Встановлено особливості використання кожного з них, переваги та недоліки. Для їх подолання і за основу розроблення методу взято модель аналізування уразливостей соціотехнічних систем. Її задано як нечіткий направлений соціальний граф, що визначається множинами екторів і відношень між ними. Це дозволило врахувати специфіку впливу соціальної інженерії при маніпулюванні користувачами соціотехнічних систем. Зокрема, виокремити різновиди екторів, відношення між ними, характеристики центральності та престижу. З огляду на це, запроновано метод аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії. Його реалізовано насамперед встановленням екторів (соціальний інженер, користувач, уразливості користувача, форми маніпулювання свідомістю); відношень між екторами; належностей відношень між екторами; характеристик екторів і відношень між ними. Серед таких характеристик виокремлено направленість, близькість, незалежність. Запропонований метод орієнтований на виявлення і протидію використанню уразливостей користувачів соціотехнічних систем. Унаслідок цього можливе встановлення вірогідних способів впливання на них з урахуванням особливостей реалізування. Їх прояв анілізується на рівнях ектора, декількох екторів, а саме: діад, тріад. Як наслідок, встановлюються умови прояву та відсутності впливів соціальної інженерії на користувачів соціотехнічних систем. Водночас їх направленість – безпосередня або опосередкована. Безпосередній вплив здійснюється без виокремлення маніпулятивної форми та орієнтований виключно на користувача. Тоді як опосередкований – характеризується визначенням їх різновиду. У перспективах подальших досліджень планується на основі запропонованого методу розробити комп’ютерну модель аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії.

**Ключові слова:** соціотехнічна система, уразливість користувача, аналізування уразливостей, метод аналізування уразливостей, соціальна інженерія, нечіткий соціальний граф.

**Постановка проблеми.** Відповідно до [1] вплив соціальної інженерії на користувачів соціотехнічних систем здійснюється через уразливості. При цьому досягається формування у них “нової” поведінки завдяки маніпулюванню, наприклад, слабкостями, потребами, маніями (пристрастями), захопленнями [2]. Тому для запобігання таким впливам соціальної інженерії запропоновано модель аналізування уразливостей користувачів як нечіткого соціального графу. Насамперед стосовно форм маніпулювання свідомістю. Отже, розроблення методу аналізування уразливостей користувачів соціотехнічних систем до впливів соціальної інженерії є актуальним.

**Аналіз останніх досліджень і публікацій.** Дослідженню впливів соціальної інженерії приділено увагу в [3] - [9]. Необхідності протидії атакам соціальної інженерії запропоновано в [3]. Показано те, що передумовою упровадження ефективних заходів є формування множини характерних ознак і складників. Така обумовленість пов'язана з обмеженістю застосування відомої класифікації атак соцальної інженерії. Введення нових ознак і складників сприяло її розширенню. Серед критеріїв виокремлено, наприклад [3], взаємодією з політикою безпеки; дистанційністю; ініціалізацією; інструментарієм; маніпулюванням; порушенням характеристик безпеки; реляційними ознаками; ступенем тяжкості; типом атакованого джерела; типом доступу; типом звернення. Передумови використання соціальної інженерії описано в [4]. Встановлено, що її запорукою є знання з інформатики, соціальної психології. Разом з тим показано наявність етичних проблем дослідження впливів соціальної інженерії. Важливість такого виокремлення обумовлена орієнтованістю на запобігання втратам. Водночас акцентовано увагу на відсутності формалізацій зазначених вимог і на важливості вирішення етичних проблем. Встановлені проблеми стосуються насамперед тестування на проникнення. Спонукання працівників організацій до протидії впливам соціальної інженерії викладено в [5]. Це досягалося завдяки розробленню відповідного опитувальника. Він поширювався серед працівників організацій з метою з'ясування ставлення до соціальної інженерії. На основі отриманих результатів встановлено існування сильного зв'язку між ставленням і прагненням протидіяти її впливам. Водночас встановлено взаємозалежність між лідерством, культурою і усвідомленням необізнаності забезпечення інформаційної безпеки. Схильність людей довіряти одна одній досліджено в [6]. Такий вибір обумовлено тлумаченням її як уразливості, через яку може реалізуватися вплив соціальної інженерії. Для запобігання експлуатуванню уразливості "схильність довіряти" ацентовано увагу на двох заходах, а саме: підвищенні обізнаності, попередженні про загрозу розголошення персональних даних. Підвердження необхідності цих заходів здійснено на основі відомостей про розголошення персональних даних (електронної пошти, номеру банківського рахунку). Водночас показано обмеженість застосування попередження про впливи соціальної інженерії. Атаки типу підробленої точки доступу та фішингової сторінки досліджено в [7]. Зокрема, зібрано та проаналізовано дані з різних джерел та наведено змістовну статистику зломів. Як організації обрано заклади вищої освіти технічного, гуманітарного і змішаного профілів. Суть проведеного есперименту полягала в розробленні для кожного з них форм реєстрації. Це дозволило змоделювати вебресурси, зокрема, дизайн говлоних сторінок. Крім того, створено стенд для проведення і збирання і аналізування статистичних даних. Загалом стало можливим визначення рівня обізнаності студентів, аспірантів. Напрями протидії використанню соціальної інеженерії в організаціях на прикладі закладів охорони здоровя викладено в [8]. Це реалізується шляхом підвищення інформаціної обізнаності працівників. Насамперед зосереджено увагу на проявах соціальної інженерії і, як наслідок, заходах їх протидії. Такий підхід орієнтований як на окремого працівника, так і організацію загалом. Так формується колективне знання, наявність якого дозволяє протидіяти впливам соціальної інженерії на працівників організацій. Методи протидії впливам соціальної інженерії проаналізовано в [9] - [12]. Серед інструментальних засобів виокремлено Social-Engineer Toolkit, Social Engineering Defensive Framework, Social Engineering Optimizer, Kali Linux. Як один з найбільш поширених методів обрано тестування на проникнення. Воно здійснюється для виявлення та запобігання есплуатуванню уразливостей користувачів соціотехнічних систем. Дане завдання виконується застосуванням таких інструментальних засобів як Social-Engineer Toolkit, Kali Linux, Cogni-Sense. Крім того, виділено два аспекти протидії використанню соціальної інженерії. Перший аспект пов'язаний з поняттям дослідження суб'кта впливу соціальної інженерії. Тоді як у межах другого виокремлюється об'єкт. Завдяки такому виділенню встановлено вірогідні сценарії впливів соціальної інженерії.

**Метою статті є** визначення способів впливу соціальної інженерії з урахуванням особливостей їх реалізування через уразливості користувачів.

**Виклад основного матеріалу дослідження.** Нечіткість поведінки як соціальних інженерів, так і користувачів соціотехнічних систем враховується завдяки використанню нечіткого направленого соціального графому [13] - [16]. Для цього введено множину впорядкованих пар елементів $V$ [1]

$$V \times V = \{(v_i, v_j) \mid v_i \in V \wedge v_j \in V\}, \quad (1)$$
$$i = \overline{1,n};\ j = \overline{1,n}.$$

З огляду на (1), модель аналізування уразливостей соціотехнічних систем представлено виразом (2)

$$\forall (v_i, v_j) \in V \times V : \underset{\sim}{\mu}_G(v_i, v_j) \in M,$$
$$\underset{\sim}{G} = \{((v_i, v_j) \mid \underset{\sim}{\mu}_G(v_i, v_j))\}, \quad (2)$$
$$\underset{\sim}{G} \subseteq V \times V,$$

де $M$ – множина належностей $(v_i, v_j)$ множини $V \times V$, $M = [0,1]$;

$\underset{\sim}{\mu}_G(v_i, v_j)$ – функція належностей $(v_i, v_j)$ множини $V \times V$.

З огляду на (1) і (2), використання методу аналізування уразливостей користувачів соціотехнічних систем до впливів соціальної інженерії починається з формування множини екторів. Вона задається шляхом об'єднання користувачів, соціальних інженерів і насамперед форм впливу. Тож отримаємо

$$V = \bigcup_{i=1}^{n} v_i .$$

де $v_i$ $i$-й ектор, наприклад [1], рис. 1:

- соціальний інженер, $v_1$;
- користувач, $v_2$;
- свідомість, $v_3$;
- маніпулювання, $v_4$;
- обман, $v_5$;
- шахрайство, $v_6$;
- афера, $v_7$;
- інтрига, $v_8$;
- містифікація, $v_9$;
- провокація, $v_{10}$

$$V = \bigcup_{i=1}^{10} v_i = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}\}.$$

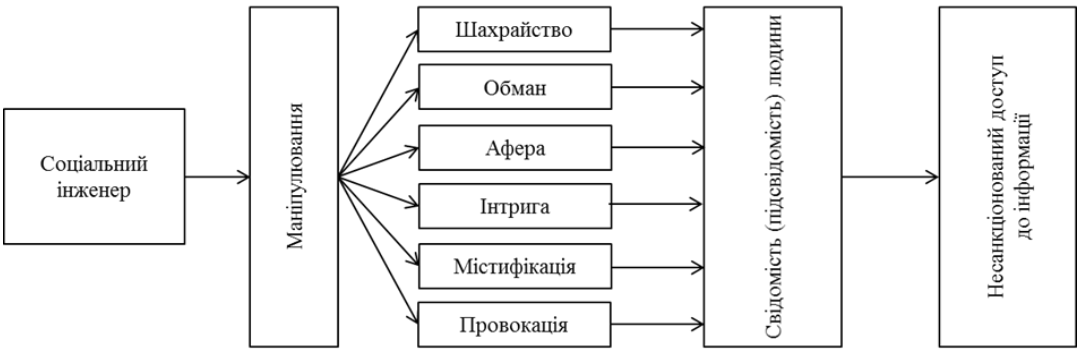


Рисунок 1 – Використання соціоінженерного підходу [9]

Оскільки вплив соціальної інженерії здебільшого реалізується за допомогою фішингу, фармінгу, смішінгу, вішінгу, спір фішінгу, вейлінгу, то в табл. 1 проаналізовано віповідність атаками соціальної інженерії і формам маніпулятивного впливу. Тож даний вплив здійснюється здебільшого завдяки шахрайству та обману. Тоді як основою для створення фіктивних ситуацій протягом прітекстінгу є афера, інтрига, містифікація та провокація [9].

Таблиця 1 – Форми впливу соціальної інженерії [9]

| № п/п | Різновид соціоінженерної атаки | Форми маніпулятивного впливу | | | | | |
|---|---|---|---|---|---|---|---|
| | | Шахрайство | Обман | Афера | Інтрига | Містифікація | Провокація |
| 1. | Фішінг | + | + | – | – | – | – |
| 2. | Фармінг | + | + | – | – | – | – |
| 3. | Прітекстінг | + | + | + | + | + | + |
| 4. | Смішінг | + | + | – | – | – | – |
| 5. | Вішінг | + | + | – | – | – | – |
| 6. | Спірфішінг | + | + | – | – | – | – |
| 7. | Вейлінг | + | + | – | – | – | – |

Після того як сформовано множину екторів необхідно визначити відношення між ними. Для цього використовується знаходження декартового добутку множини екторів $V$, як наслідок отримаємо:

$$V \times V = \{(v_1, v_1), (v_1, v_2), (v_1, v_3), ..., (v_1, v_j), ..., (v_1, v_n); ...\}.$$

Кожен з елементів множини $V \times V$ є впорядкованою парою, якою характеризується наявність або відсутність відношення між двома екторами. До того ж ними представляється направленість від $i$ до $j$ ектора, наприклад [1], $(v_1, v_5)$ – від соціального інженера (ектор $v_1$), до обману (ектор $v_5$) як маніпулятивної форми). При цьому соціальний інженер тлумачиться відправником, обман – отримувачем. Така направленість може бути або відсутньою, або асиметричною. Прикладом останньої є дуга $(v_1, v_5)$. Тоді як відсутність направленості характерна для впорядкованої пари $(v_2, v_5)$ – користувач соціотехнічної системи (ектор $v_2$) – обман (ектор $v_5$).

Крім того, можливе визначення числа вхідних та вихідних дуг. Воно дозволяє встановити направленість між екторами та, як наслідок, їх різновид [1], [14]:

– ізольований, $d_I(v_i) = d_O(v_i) = 0$. Наприклад, соціальний інженер не застосовує жодну з маніпулятивних форм, $v_1$ – $d_I(v_1) = d_O(v_1) = 0$;

– відправник, $d_I(v_i) = 0$, $d_O(v_i) > 0$. Наприклад, соціальний інженер (ектор $v_1$) впливає через маніпулятивні форми на користувача соціотехнічної системи (ектор $v_2$), $d_I(v_1) = 0$, $d_O(v_1) = 1 > 0$

– отримувач, $d_I(v_i) > 0$, $d_O(v_i) = 0$. Наприклад, на користувача (ектор $v_2$) соціотехнічної системи через його вразливості впливає соціальний інженер $d_I(v_1, v_2, v_5, v_6, v_7, v_8, v_9, v_{10}) = 5 > 0$, $d_O(v_i) = 0$.

Після того як задано відношення між екторами переходимо до визначення характеристик центральності та престижу [13], [14]. Так, активність ектора встановлюється характеристикою центральності, наприклад: маніпулятивна форма (шахрайство), уразливість користувача соціотехнічної системи. Вона визначається ступенем і близькістю. Ступінь центральності знаходиться за такою рівністю [1], [14]

$$C'_D(v_i) = \frac{\sum_{j=1}^{n} \mu_{\tilde{G}}(v_i, v_j)}{n-1}.$$

Тоді як близькість між двома екторами встановлюється з огляду на відстань між ними [1], [14]

$$C'_C(v_i) = \frac{J_i / n-1}{\sum_{j=1}^{n} d(v_i, v_j) \Big/ J_i},$$

де $J_i$ – кількість екторів у межах впливу ектора $v_i$, наприклад, користувачів соціотехнічної системи, $d(v_i, v_j)$ – відстань між екторами $v_i$ та $v_j$, наприклад, між соціальним інженером і користувачем соціотехнічної системи.

За аналогією з центральністю для визначення престижу екторів використовується ступінь і близькість. Ступенем престижу характеризується незалежність кожного з екторів. Його ступінь визначається [1]

$$P_D(v_i) = \frac{d_I(v_i)}{n-1}.$$

де $d_I(v_i)$ – кількість екторів, що пов'язані з ектором $v_i$, наприклад, кількість маніпулятивних форм соціального інженера, що реалізуються через уразливість користувача соціотехнічної системи.

Близькістю престижу характеризується кількість екторів, що безпосередньо (уразливість – користувач соціотехнічної системи) або опосередковано (маніпулятивна форма – уразливість – користувач соціотехнічної системи) пов'язані з ектором $v_j$ [1].

$$P_P(v_i) = \frac{I_i / n-1}{\sum_{j=1}^{n} d(v_j, v_i) \Big/ I_i},$$

де $I_i$ – кількість екторів у межах впливу ектора $v_i$.

Використання (3) дозволяє аналізувати вразливості соціотехнічних систем на рівні ектора, пари екторів (діада), тріад [14]. Для цього кожен з рівнів відображається підграфом $\tilde{G}_s$

$$\tilde{G}_s \subseteq \tilde{G}.$$

Відношення між двома екторами відображається діадою як підграфом. Це означає, що він має, наприклад, дві вершини та дугу між ними. Кожна з впорядкованих пар вершин може знаходиться у одному з двох станів і відображає, наприклад:

– вплив соціального інженера (ектор $v_1$) на користувача соціотехнічної системи (ектор $v_2$)

$$\tilde{G}_s = \{((v_1, v_2) \mid \mu_{\tilde{G}}(v_1, v_2))\};$$

– відсутність впливу соціального інженера (ектор $v_1$) на користувача соціотехнічної системи (ектор $v_2$)

$$\tilde{G}_s = \{((v_1, v_2) \mid 0)\}.$$

Відношення між трьома екторами представляється підграфом і називається тріадою. Має три вершини та дуги між ними. Може перебувати в одному в декількох станах і відображає, наприклад [1]:

– безпосередній або опосередкований вплив соціального інженера (ектор $v_1$) без або з урахуванням обману як маніпулятивної форми (ектор $v_5$) на користувача соціотехнічної системи (ектор $v_2$)

$$\underset{\sim}{G_s} = \{((v_1, v_5) \mid \underset{\sim}{\mu_G}(v_1, v_5)), ((v_1, v_2) \mid \underset{\sim}{\mu_G}(v_1, v_2)), ((v_5, v_2) \mid \underset{\sim}{\mu_G}(v_5, v_2))\};$$

– опосередкований вплив соціального інженера (ектор $v_1$) з урахуванням обману як маніпулятивної форми (ектор $v_5$) на користувача соціотехнічної системи (ектор $v_2$)

$$\underset{\sim}{G_s} = \{((v_1, v_5) \mid \underset{\sim}{\mu_G}(v_1, v_5)), ((v_1, v_2) \mid 0), ((v_5, v_2) \mid \underset{\sim}{\mu_G}(v_5, v_2))\};$$

– безпосередній вплив соціального інженера (ектор $v_1$) на користувача соціотехнічної системи (ектор $v_2$)

$$\underset{\sim}{G_s} = \{((v_1, v_5) \mid 0), ((v_1, v_2) \mid \underset{\sim}{\mu_G}(v_1, v_2)), ((v_5, v_2) \mid 0)\}.$$

**Висновки.** Отже, запропоновано метод аналізування уразливостей користувачів соціотехнних систем до впливів соціальної інженерії. Його використання дозволяє встановити множину екторів, якими характеризуються або соціальні інженери, або користувачі соціотехнчної системи, або форми маніпулятивного впливу. Встановленням відношень між ними визначено вірогідні зв'язки та, як наслідок, способи впливу соціальної інженерії на користувачів.

Використання запропонованого методу дозволяє досліджувати як окремих екторів, так і їх груп, наприклад, діад, тріад. Водночас встановлюати особливості впливу на користувача: безпосередній, опосередкований, безпосередній або опосередкований. Крім того, виокремлено різновиди екторів з боку соціального інженера, користувача, маніпулятивної форми, уразливості за числами вхідних і вихідних дуг. Тоді як важливість кожного з них оцінено за допомогою характеристик центральності та престижу.

У перспективах подальших досліджень планується на основі запропонованого методу розробити комп'ютерну модель аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії**.**

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В. В. Мохор, О. В. Цуркан, Р. П. Герасимов, О. М. Крук та В. О. Покровська, "Модель аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії", *Кібербезпека: освіта, наука, техніка*, т. 4, № 8, с. 165-173, 2020, doi: https://doi.org/10.28925/2663-4023.2020.8.165173.

[2] V. V. Mokhor, O. V. Tsurkan, R. P. Herasymov, and V. V. Tsurkan, "Information Security Assessment of Computer Systems by Socio-engineering Approach", *Selected Papers of the XVII International Scientific and Practical Conference Information Technologies and Security*, vol. 2067. Aachen, Germany: CEUR Workshop Proceedings, 2017, pp. 92-98. [Online]. Available: http://ceur-ws.org/Vol-2067/paper13.pdf. Accessed on: February 12, 2020.

[3] О. Г. Корченко, Д. А. Горніцька, та А. Ю. Гололобов, "Розширена класифікація методів соціального інжинірингу", *Безпека інформації*, т. 20, № 2, с. 197-205, 2014, doi: https://doi.org/10.18372/2225-5036.20.7308.

[4] F. Mouton, M. M. Malan, K. K. Kimppa, and H. S. Venter, "Necessity for ethics in social engineering research", *Computers & Security*, vol. 55, pp. 114-127, 2015, doi: http://dx.doi.org/10.1016/j.cose. 2015.09.0010167-4048.

[5] W. R. Flores, and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness", *Computers & Security*, vol. 59, pp. 26-44, 2016, doi: http://dx.doi.org/doi: 10.1016/j.cose.2016.01.004.

[6] M. Junger, L. Montoya, F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks", *Computers in Human Behavior*, vol. 66, pp. 75-87, 2017, doi: http://dx.doi.org/ 10.1016/j.chb.2016.09.012.

[7] В. Ю. Соколов, та Д. М. Курбанмурадов, "Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності", *Кібербезпека: освіта, наука, техніка*, т. 1, № 1, с. 6-16, 2018, doi: https://doi.org/10.28925/2663-4023.2018.1.616.

[8] N. Abe, and M. Soltys, "Deploying Health Campaign Strategies to Defend Against Social Engineering Threats", Procedia Computer Science, vol. 159, pp. 824-831, 2019, doi: https://doi.org/10.1016/ j.procs.2019.09.241.

[9] О. Цуркан, Р. Герасимов, та О. Крук, "Методи протидії використанню соціальної інженерії", *Information Technology and Security*, vol. 7, iss. 2 (13), pp. 161-170, July-December 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190563.

[10] F. Mouton, L. Leenen, and H. Venter, "Social engineering attack examples, templates and scenarios", *Computers & Security*, vol. 59, pp. 1-54, June 2016, doi: https://doi.org/ 10.1016/j.cose. 2016.03.004.

[11] F.-F. M. Amir, H.-K. Mostafa, and T.-M. Reza, "The Social Engineering Optimizer (SEO)", *Engineering Applications of Artificial Intelligence*, vol. 72, pp. 267-293, 2018, doi: https://doi.org/10.1016/j.engappai.2018.04.009.

[12] О. В. Цуркан, та Т. М. Клименко, "Аналіз вразливостей соціотехнічних систем на основі нечітких соціальних графів", на *Науково-практичній конференції Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України Безпека енергетики в епоху цифрової трансформації*, Київ, 2019, с. 28.

[13] O. V. Tsurkan, R. P. Herasymov, and O. M. Kruk, "Presentation the interaction of the subject and the object of socio-engineering influence with a social graph", in *Proc. Fourth International Scientific and Technical Conference Computer and Informational Systems and Technologies*, Kharkiv, 2020, pp. 46, doi: https://doi.org/10.30837/IVcsitic2020201371.

[14] J. N. Moderson, and P. S. Nair, *Fuzzy Graphs and Fuzzy Hypergraphs*. Heidelberg, Germany: Physica-Verlag Heidelberg, 2000, doi: https://doi.org/10.1007/978-3-7908-1854-3.

[15] L. Zadeh, Fundamentals of a new approach to the analysis of complex systems and decision-making processes. *Matematika segodnja*, Moscow, Russia: Znanie, 1974, pp. 5-49.

[16] S. Wasserman, and K. Faust, *Social Network Analysis: Methods and Applications*. Cambridge, England: Cambridge University Press, 2012, doi: https://doi.org/10.1017/CBO9780511815478.

Стаття надійшла до редакції 26.02.2020.

## REFERENCE

[1] V. Mokhor, O. Tsurkan, R. Herasymov, O. Kruk, and V. Pokrovska, "Model of vulnerabilities analysis of socio-technical systems to the social engineering influences", *Cybersecurity: Education, Science, Technique*, vol. 4, no. 8, pp. 165-173, 2020, doi: https://doi.org/ 10.28925/2663-4023.2020.8.165173.

[2] V. V. Mokhor, O. V. Tsurkan, R. P. Herasymov, and V. V. Tsurkan, "Information Security Assessment of Computer Systems by Socio-engineering Approach", *Selected Papers of the XVII International Scientific and Practical Conference Information Technologies and Security*, vol. 2067. Aachen, Germany: CEUR Workshop Proceedings, 2017, pp. 92-98. [Online]. Available: http://ceur-ws.org/Vol-2067/paper13.pdf. Accessed on: February 12, 2020.

[3] O. G. Korchenko, D. A. Gornitska, and A. Yu. Gololobov, "Extended classification of methods of social engineering", *Ukrainian Scientific Journal of Information Security*, vol. 20, no. 2, pp. 197-205, 2014, doi: https://doi.org/10.18372/2225-5036.20.7308.

[4] F. Mouton, M. M. Malan, K. K. Kimppa, and H. S. Venter, "Necessity for ethics in social engineering research", *Computers & Security*, vol. 55, pp. 114-127, doi: http://dx.doi.org/10.1016/j.cose.2015.09. 0010167-4048.
[5] W. R. Flores, and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness", *Computers & Security*, vol. 59, pp. 26-44, 2016, doi: http://dx.doi.org/10.1016/j.cose.2016.01.004.
[6] M. Junger, L. Montoya, F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks", *Computers in Human Behavior*, vol. 66, pp. 75-87, 2017, doi: http://dx.doi.org/ 10.1016/j.chb.2016.09.012.
[7] V. Y. Sokolov, and D. M. Kurbanmuradov, "Method of Counteraction in Social Engineering on Information Activity Objectives", *Cybersecurity: Education, Science, Technique*, vol. 1, no. 1, pp. 6-16, 2018, doi: https://doi.org/10.28925/2663-4023.2018.1.616.
[8] N. Abe, and M. Soltys, "Deploying Health Campaign Strategies to Defend Against Social Engineering Threats", Procedia Computer Science, vol. 159, pp. 824-831, 2019, doi: https://doi.org/10.1016/ j.procs.2019.09.241.
[9] O. Tsurkan, R. Herasymov, and O. Kruk, "Methods of counteracting social engineering", *Information Technology and Security*, vol. 7, iss. 2 (13), pp. 161-170, July-December 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190563.
[10] F. Mouton, L. Leenen, and H. Venter, "Social engineering attack examples, templates and scenarios", *Computers & Security*, vol. 59, pp. 1-54, June 2016, doi: https://doi.org/ 10.1016/j.cose. 2016.03.004.
[11] F.-F. M. Amir, H.-K. Mostafa, and T.-M. Reza, "The Social Engineering Optimizer (SEO)", *Engineering Applications of Artificial Intelligence*, vol. 72, pp. 267-293, 2018, doi: https://doi.org/10.1016/j.engappai.2018.04.009.
[12] O. V. Tsurkan, and T. M. Klymenko, "Vulnerability analysis of sociotechnical systems based on fuzzy social graphs", in *Proc. Scientific and Practical Conference of Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine Energy security in the era of digital transformation*, Kyiv, 2019, pp. 28.
[13] O. V. Tsurkan, R. P. Herasymov, and O. M. Kruk, "Presentation the interaction of the subject and the object of socio-engineering influence with a social graph", in *Proc. Fourth International Scientific and Technical Conference Computer and Informational Systems and Technologies*, Kharkiv, 2020, pp. 46, doi: https://doi.org/10.30837/IVcsitic2020201371.
[14] J. N. Moderson, and P. S. Nair, *Fuzzy Graphs and Fuzzy Hypergraphs*. Heidelberg, Germany: Physica-Verlag Heidelberg, 2000, doi: https://doi.org/10.1007/978-3-7908-1854-3.
[15] L. Zadeh, Fundamentals of a new approach to the analysis of complex systems and decision-making processes. *Matematika segodnja*, Moscow, Russia: Znanie, 1974, pp. 5-49.
[16] S. Wasserman, and K. Faust, *Social Network Analysis: Methods and Applications*. Cambridge, England: Cambridge University Press, 2012, doi: https://doi.org/10.1017/CBO9780511815478.

ROSTYSLAV HERASYMOV,
OLHA KRUK,
OKSANA TSURKAN,
VADYM YASHENKOV

**METHOD OF VULNERABILITIES ANALYSIS OF SOCIO-TECHNICAL SYSTEMS TO THE SOCIAL ENGINEERING INFLUENCES**

The influence of social engineering on users of sociotechnical systems is investigated. To prevent such influence, an analysis of their vulnerabilities to forms of consciousness manipulation is proposed. Typical approaches to counter the use of social engineering are highlighted and compared. The features of using each of them, their advantages and disadvantages are established. To overcome

them, and as a basis for the development of the method, a model for analyzing the vulnerabilities of sociotechnical systems is taken. It is defined as a fuzzy directed social graph, determined by the sets of actors and relations between them. This made it possible to consider the specifics of social engineering influence when manipulating users of sociotechnical systems. It allowed us to identify the variety of actors, the relations between them, the characteristics of centrality and prestige. Given this, a method of analyzing the vulnerabilities of sociotechnical systems to the social engineering impacts is proposed. It is realized first by actors' emplacement (social engineer, user, user vulnerabilities, mind manipulation forms); relations between actors; affiliations of relations between actors; characteristics of actors and relations between them. Among such characteristics, directionality, proximity, independence are highlighted. The proposed method is focused on identifying and counteracting the use of sociotechnical systems users' vulnerabilities. As a result, it is possible to establish potential ways of influence on them, taking into account the implementation features. Their manifestation is analyzed at the levels of an actor, several actors, namely: dyad, triad. As a result, the conditions for the manifestation and absence of social engineering influence on sociotechnical systems users are established. At the same time, their focus is direct or indirect. The direct impact is carried out without highlighting the manipulative form and is aimed exclusively at the user. While indirect – characterized by the definition of their variety. In future research, it is planned based on the proposed method to develop a computer model for analyzing the sociotechnical system's vulnerabilities to the influences of social engineering.

**Keywords:** sociotechnical system, user vulnerability, vulnerability analysis, vulnerability analysis method, social engineering, fuzzy social graph.

**Герасимов Ростислав Павлович**, науковий співробітник, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

ORCID: 0000-0002-4115-8344.

E-mail: gerasimov.rostislav@gmail.com.

**Крук Ольга Миколаївна**, молодший науковий співробітник, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

ORCID: 0000-0003-2994-6804.

E-mail: o.n.kruk@gmail.com.

**Цуркан Оксана Володимирівна**, молодший науковий співробітник, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

ORCID: 0000-0002-5524-8834.

E-mail: o.tsurkan24@gmail.com.

**Яшенков Вадим Петрович**, науковий співробітник, Інститут електрозварювання ім. Є.О. Патона Національної академії наук України, Київ, Україна.

ORCID 0000-0002-9015-1181.

E-mail: vadym.yashenkov@gmail.com.

**Herasymov Rostyslav**, researcher, Pukhov institute for modeling in energy engineering of the National academy of sciences of Ukraine, Kyiv, Ukraine.

**Kruk Olha**, junior researcher, Pukhov institute for modeling in energy engineering of the National academy of sciences of Ukraine, Kyiv, Ukraine.

**Tsurkan Oksana**, junior researcher, Pukhov institute for modeling in energy engineering of the National academy of sciences of Ukraine, Kyiv, Ukraine.

**Yashenkov Vadym**, academic expert, E. O. Paton electric welding institute of the National academy of sciences of Ukraine, Kyiv, Ukraine.