КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№4 (8), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.8.165173
УДК 004.056.53::519.171

Мохор Володимир Володимирович
член-кореспондент НАН України, д.т.н., професор, директор
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна
ORCID: 0000-0001-5419-9332
v.mokhor@gmail.com

Цуркан Оксана Володимирівна
молодший науковий співробітник
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна
ORCID:0000-0002-5524-8834
o.tsurkan24@gmail.com

Герасимов Ростислав Павлович
науковий співробітник
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна
ORCID: 0000-0002-4115-8344
gerasimov.rostislav@gmail.com

Крук Ольга Миколаївна
молодший науковий співробітник
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна
ORCID: 0000-0003-2994-6804
o.n.kruk@gmail.com

Покровська Валерія Олександрівна
інженер лабораторії
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
ORCID: 0000-0002-1318-5521
Hilariyap@gmail.com

МОДЕЛЬ АНАЛІЗУВАННЯ УРАЗЛИВОСТЕЙ СОЦІОТЕХНІЧНИХ СИСТЕМ ДО ВПЛИВІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Анотація. Розглянуто соціотехнічні системи як утворення з технічної і соціальної підсистем. Встановлено напрями забезпечення їх безпеки та серед них виокремлено використання технічних можливостей з урахуванням поведінки користувачів. Приділено увагу їх вразливостям до реалізування соціотехнічних загроз, зокрема, впливів соціальної інженерії. Показано орієнтованість такого впливу на маніпулювання слабкостями, потребами, маніями (пристрастями), захопленнями користувачів. Це призводить до неспроможності соціотехнічних систем протидіяти впливанню соціальної інженерії. Запобігання цьому можливе завдяки аналізуванню уразливостей користувачів стосовно форм маніпулювання їх свідомістю. Зіставлено підходи до протидії використанню соціальної інженерії. Для кожного з них проаналізовано особливості застосування, переваги та недоліки. З огляду на це запропоновано використання нечітких направлених соціальних графів для задання моделі аналізування уразливостей соціотехнічних систем. Цьому передувало визначення понять соціальної мережі, ектора, відношення. Таке представлення дозволило врахувати особливості впливання соціальної інженерії. Зокрема, числами вхідних і вихідних дуг виокремлено різновиди екторів з боку соціального інженера, користувача, маніпулятивної форми, уразливості. Тоді як важливість кожного з них визначено за допомогою характеристик центральності та престижу. Водночас виокремлено рівні ектора, діади, тріади аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії. Це дозволить визначати способи таких впливів з урахуванням особливостей їх реалізування через уразливості користувачів і, як наслідок, протидіяти їм. У перспективах подальших досліджень планується на

основі запропонованої моделі розробити метод аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії.

Ключові слова: соціотехнічна система; аналізування уразливостей, соціальна інженерія, нечіткий соціальний граф.

1. ВСТУП

Під соціотехнічними системами розуміються утворення з технічної і соціальної підсистем. Технічна підсистема відображається набором апаратного, програмного забезпечення. Їх використання дозволяє користувачам соціотехнічних систем перетворювати вхідні дані у вихідні. Тоді як до соціальної підсистеми належать користувачі – працівники організації, їх знання, уміння і навики. Кожна з виокремлених складових взаємодіє одна з одною через зовнішнє середовище, зокрема, організацію [1], [2], [3]. Тому, з одного боку [2], соціотехнічні системи розробляються на принципах інноваційності, розвивання людських ресурсів, гнучкості зв'язку зі зовнішнім середовищем. З іншого [1] – як об'єкти інформатизації з прийнятним ризиком реалізування загроз її підсистемам. Тож безпека соціотехнічних систем забезпечується за двома напрямами, а саме [3], [4]: використання технічних можливостей без урахування поведінки користувачів; використання технічних можливостей з урахуванням поведінки користувачів. Як наслідок, у межах другого напряму об'єктом забезпечення безпеки є користувачі як ключові елементи соціотехнічних систем [4]. При цьому акцентується увага на їх уразливостях до реалізування соціотехнічних загроз [5], зокрема, впливів соціальної інженерії [6].

Постановка проблеми. Використання соціальної інженерії впливає на користувачів соціотехнічних систем через їх уразливості. Серед них виокремлюються слабкості, потреби, манії (пристрасті), захоплення. Маніпулювання даними вразливостями орієнтоване на спонукання користувачів до нової моделі поведінки та, як наслідок, отримання "несанкціонованого" доступу до інформації. Це призводить до неспроможності соціотехнічних систем протидіяти впливанню соціальної інженерії [7], [8]. Запобігання цьому можливе завдяки аналізуванню уразливостей користувачів до форм маніпулювання свідомістю, наприклад [9], шахрайство, обман, афера, інтрига, містифікація.

Аналіз останніх досліджень і публікацій. Дослідженню використання соціальної інженерії приділено увагу в [7] - [14]. Оцінювання захищеності інформації у комп'ютерних системах за соціоінженерним підходом розглянуто в [7]. Даний підхід застосовано до користувачів як основного об'єкта впливання соціальної інженерії. Завдяки цьому можливе оцінювання і розроблення способів підвищення захищеності комп'ютерних систем з урахуванням людського фактору. В [8] розкрито метод протидії використанню соціальної інженерії. При цьому встановлено переваги та недоліки відомих методів і запропоновано взяти за основу їх подолання маніпулятивну форму соціоінженерного впливу [9]. Інформаційну модель користувача стосовно реалізування загрози соціоінженерної атаки побудовано в [10]. Нею відображено його ім'я, прізвище, посаду, належність до групи користувачів, дозволи на дії і доступ до інформаційних об'єктів. Побудованою моделлю описуються вірогідні соціоінженерні загрози безпеці користувачів без урахування особливостей їх реалізування. Соціальну інженерію як перспективний метод кіберрозвідки розглянуто в [11]. Його використання орієнтоване на отримання інформації про інформаційно-телекомунікаційну систему неавторизованим

користувачем через людський фактор. Множину характерних ознак і складових соціоінженерних атак визначено в [12]. Завдяки цьому розширено їх класифікацію для розроблення ефективних засобів протидії. Способи маніпулювання користувачами проаналізовано в [13]. Зокрема, приклади, шаблони та вірогідні сценарії їх реалізування. При цьому основним твердженням стало орієнтованість на користувачів як слабку ланку забезпечення інформаційної безпеки. Суб'єкта (або нападника) та об'єкта (або захисника) впливання соціальної інженерії виокремлено в [14]. Дії нападника зведено до використання її шаблонів і сценаріїв з прагненням перемогти захисника.

Отже, розроблення моделі аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії є актуальним.

Мета статті. Встановлення особливостей впливання соціальної інженерії через уразливості соціотехнічних систем на забезпечення їх безпеки.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Уразливості соціотехнічних систем до впливів соціальної інженерії аналізуються з огляду на відношення між соціальним інженером і користувачем. Така структура між даними індивідами тлумачиться як соціальна мережа. Нею відображається орієнтованість впливу соціального інженера на користувача соціотехнічної системи, наприклад, входження в довіру для отримання доступу до інформації. З огляду на це основними поняттями є [7], [9], [15]:

Соціальна мережа – кінцева множина або множини екторів з реляційними відношеннями між ними.

Ектор – соціальний суб'єкт, який може здатний або не здатний до діяльності. Як ектори розглядаються соціальний інженер, користувач, уразливості користувача, форми маніпулювання свідомістю.

Відношення – взаємозв'язок між парою екторів (наприклад, "соціальний інженер – користувач"), яким визначаються соціальні відносини між ними. За їх допомогою, наприклад, можливе представлення оцінювання соціальним інженером користувача (висловлення доброзичливості, дружелюбності, розгубленості, авторитетності); передавання інформаційних ресурсів каналами зв'язку (повідомлень електронною поштою); належності користувача соціотехнічної системи (відділ, служба організації); поведінкових відносин (міжособистісне спілкування, надсилання повідомлень електронною поштою, спілкування телефоном); формальних відносин (керівник, підлеглий, клієнт, знайомий).

Відношення між соціальним інженером і користувачем соціотехнічної системи відображаються таким соціальним графом [16]

$$G = (V, E) \tag{1}$$

де V – множина екторів, E – множина дуг між парами екторів.

Однак, використання даного підходу на практиці обмежується складністю чітких міркувань стосовно поведінки як соціального інженера, так і користувача соціотехнічної системи [17]. Це обумовлено, по-перше, різноманітністю існування і реалізування способів впливання соціальної інженерії. По-друге, неоднозначністю поведінки користувача соціотехнічної системи залежно від маніпулятивної форми впливання на нього з боку соціального інженера.

ISSN 2663 - 4023

Для врахування і, як наслідок подолання цих обмежень використано підхід, що запропоновано в [18]. За основу взято твердження про нечіткість мислення людини. Це означає, що його елементи належать до нечітких класів об'єктів. При цьому перехід від належності до неналежності класу неперервний. Ступінь такого переходу визначається функцією належності. Тому для врахування цих особливостей використовується логіка з нечіткою істинністю, нечіткими відношенням, нечіткими правилами виведення. Застосування нечіткої логіки обумовлюється здатністю до обирання важливої інформації залежно від проблемної ситуації.

З огляду на це аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії відображається нечітким направленим соціальним графом [17], [19]. Його використання дозволяє врахувати нечіткість поведінки як соціального інженера, так і користувача соціотехнічної системи.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Розглянемо множину впорядкованих пар елементів множини V, що визначаються декартовим добутком

$$V \times V = \{(v_i, v_j) \mid v_i \in V \wedge v_j \in V\}, \quad (2)$$
$$i = \overline{1,n}; \; j = \overline{1,n}.$$

Тоді модель аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії задається нечітким направленим соціальним графом G [17], [19], [20]. Під ним розуміється підмножина множини декартового добутку (2)

$$\forall (v_i, v_j) \in V \times V : \mu_G(v_i, v_j) \in M,$$
$$G = \{((v_i, v_j) \mid \mu_G(v_i, v_j))\}, \quad (3)$$
$$G \subseteq V \times V,$$

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

Кожна впорядкована пара тлумачиться дугою і нею відображається направленість від i до j ектора (наприклад, (v_1, v_2) – від соціального інженера (ектор v_1), до обману (ектор v_2) 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_2). Тоді як відсутність направленості характерна для впорядкованої пари (v_3, v_2) – користувач соціотехнічної системи (ектор v_3) – обман (ектор v_2).

Крім цього направленість між екторами враховується шляхом визначення числа вхідних та вихідних дуг між ними, а саме [19]:

$$d_I(v_i), \; (v_j, v_i) \; v_j \in V;$$
$$d_O(v_i), \; (v_i, v_j) \; v_j \in V.$$

Числа вхідних і вихідних дуг використовуються для визначення різновиду ектора при аналізуванні вразливостей соціотехнічних систем до впливів соціальної інженерії:

ISSN 2663 - 4023

– ізольований, $d_I(v_i) = d_O(v_i) = 0$. Наприклад, соціальний інженер не застосовує маніпулятивну форму v_i;

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

– отримувач, $d_I(v_i) > 0$, $d_O(v_i) = 0$. Наприклад, на користувача (ектор v_i) соціотехнічної системи через його вразливості впливає соціальний інженер.

Важливість екторів виявляється завдяки використанню характеристик центральності та престижу [17], [19]. Серед них найбільш активні ектори характеризуються центральністю, наприклад: маніпулятивна форма, уразливість користувача соціотехнічної системи. Вона визначається ступенем і близькістю. Ступінь центральності знаходиться за такою рівністю

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

Тоді як близькість між двома екторами встановлюється з огляду на відстань між ними

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

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.

У даному випадку зосереджуються на виборі екторів. Однак, поза їх увагою залишається обумовленість таких активностей як відправник або як отримувач. Дана особливість враховується характеристикою престижності. Тому нею відображаються, наприклад, або вразливості користувача, або користувач соціотехнічної системи. Це означає, що кожен з них тлумачиться як ектор отримувач. За аналогією з центральністю для визначення престижу екторів використовується ступінь і близькість.

Ступенем престижу характеризується незалежність кожного з екторів. Це означає, що престижними екторами порівно з іншими отримується багато нагород і можливостей. Його ступінь визначається

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

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.

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

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 [19]. Для цього кожен з рівнів відображається підграфом G_s

$$G_s \subseteq G.$$

Діада задається підграфом, що має дві вершини та дугу між ними. При цьому впорядкована пара вершин може знаходиться у одному з двох станів і відображає, наприклад:

– вплив соціального інженера (ектор v_1) на користувача соціотехнічної системи (ектор v_3)

$$G_s = \{((v_1, v_3) \mid \mu_G(v_1, v_3))\};$$

– відсутність впливу соціального інженера (ектор v_1) на користувача соціотехнічної системи (ектор v_3)

$$G_s = \{((v_1, v_3) \mid 0)\}.$$

Тріада представляється підграфом, що має три вершини та дуги між ними. Може перебувати в одному в декількох станах і відображає, наприклад:

– безпосередній або опосередкований вплив соціального інженера (ектор v_1) без або з урахуванням обману як маніпулятивної форми (ектор v_2) на користувача соціальної мережі (ектор v_3)

$$G_s = \{((v_1, v_2) \mid \mu_G(v_1, v_2)), ((v_1, v_3) \mid \mu_G(v_1, v_3)), ((v_2, v_3) \mid \mu_G(v_2, v_3))\};$$

– опосередкований вплив соціального інженера (ектор v_1) з урахуванням обману як маніпулятивної форми (ектор v_2) на користувача соціальної мережі (ектор v_3)

$$G_s = \{((v_1, v_2) \mid \mu_G(v_1, v_2)), ((v_1, v_3) \mid 0), ((v_2, v_3) \mid \mu_G(v_2, v_3))\};$$

– безпосередній вплив соціального інженера (ектор v_1) на користувача соціальної мережі (ектор v_3)

$$G_s = \{((v_1, v_2) \mid 0), ((v_1, v_3) \mid \mu_G(v_1, v_3)), ((v_2, v_3) \mid 0)\}.$$

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, задання моделі аналізування уразливостей соціотехнних систем нечітким направленим соціальним графом дозволило встановити особливості впливання соціальної інженерії. Для цього визначено множину екторів (соціальний інженер, маніпулятивна форма, уразливість, користувач) та впорядковані пари її елементів з функціями їх належності. Виокремлено різновиди екторів з боку соціального інженера, користувача, маніпулятивної форми, уразливості за числами вхідних і вихідних дуг. Тоді як важливість кожного з них отримано за допомогою характеристик центральності та престижу. Крім цього, встановлено рівні ектора, діади, тріади для аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії. Це дозволить

визначати способи таких впливів з урахуванням особливостей їх реалізування через уразливості користувачів і, як наслідок, протидіяти їм.

У перспективах подальших досліджень планується на основі запропонованої моделі розробити метод аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії**.**

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] С. В. Волобуев, *Безопасность социотехнических систем*. Обнинск, Россия: Викинг, 2012.

[2] Г. А. Остапенко, и Е. А. Мешкова, *Информационные операции и атаки в социотехнических системах*. Москва, Россия: Горячая линия-Телеком, 2016.

[3] А. В. Дудатьев, В. А. Лужецкий, и Д. А. Коротаев, "Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны", *Восточно-Европейский журнал передовых технологий*, т. 2, № 2 (80), с. 4-11, 2016. doi: 10.15587/1729-4061.2016.65691

[4] С. И. Кравченко, "Безопасность социотехнических систем", *НБИ технологии*, т. 12, № 2, с. 20-24, 2018. doi: 10.15688/NBIT.jvolsu.2018.2.3.

[5] Д. А. Горницкая, А. Г. Корченко, та В. П. Харченко, "Система социотехнических атак в информационной среде", на *Второй международной научно-практической конференции Проблемы экономики и управления на железнодорожном транспорте*, Киев, 2007, с. 137-138.

[6] ДП "УкрНДНЦ". (2016, Груд. 27). *ДСТУ ISO/IEC 27032. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT)*. Київ, 2018, 50 с.

[7] 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*, Kyiv, 2017, pp. 92-98. [Online]. Available: http://ceur-ws.org/Vol-2067/paper13.pdf. Accessed on: February 12, 2020.

[8] 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: 10.20535/2411-1031.2019.7.2.190563.

[9] В. В. Мохор, О. В. Цуркан, та Р. П. Герасимов, "Маніпулятивна форма соціоінженерного впливу на особистість в кіберпросторі", на *Науково-практичній конференції Актуальні проблеми управління інформаційною безпекою держави*, Київ, 2015, с. 303-304.

[10] А. Л. Тулупьев, А. Е. Пащенко, и А. А. Азаров, "Информационная модель пользователя, находящегося под угрозой социоинженерной атаки", Тр. СПИИ-РАН, вып. 13, с. 143-155, 2010.

[11] В. Л. Бурячок, О. Г. Корченко, та Л. В. Бурячок, "Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем", *Захист інформації*, т. 14, № 4 (57), с. 5-12, 2012. doi: 10.18372/2410-7840.14.3471.

[12] 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: 10.18372/2225-5036.20.7308.

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

[14] 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: 10.1016/j.engappai.2018.04.009.

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

[16] 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: 10.30837/IVcsitic2020201371.

[17] 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.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (8), 2020
ISSN 2663 - 4023

Volodymyr V. Mokhor
Corresponding Member of the NAS of Ukraine, Doctor of Technical Sciences, Professor, Director
Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0001-5419-9332
v.mokhor@gmail.com

Oksana V. Tsurkan
Junior Researcher
Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0002-5524-8834
o.tsurkan24@gmail.com

Rostyslav P. Herasymov
Researcher
Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0002-4115-8344
gerasimov.rostislav@gmail.com

Olha M. Kruk
Junior Researcher
Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0003-2994-6804
o.n.kruk@gmail.com

Valeriia O. Pokrovska
Laboratory Engineer
Institute of Special Communication and Information Protection of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: 0000-0002-1318-5521
Hilariyap@gmail.com

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

Abstract. Socio-technical systems as education with technical and social subsystems are considered. The directions for ensuring their safety have been established and among them the use of technical capabilities has been singled out, taking into account user behavior. Attention is paid to their vulnerabilities to the realisability of sociotechnical threats, in particular, the influence of social engineering. The orientation of such an influence on the manipulation of weaknesses, needs, mania (passions), user hobbies is shown. This leads to the insolvency of socio-technical systems to counteract the influence of social engineering. This can be prevented by analyzing the user's vulnerabilities regarding the forms of manipulation of their consciousness. The approaches to counteracting the use of social engineering are compared. For each of them, the application features, advantages, and disadvantages are analyzed. Given this, it is proposed to use fuzzy directed social graphs to set a model for analyzing the vulnerabilities of socio-technical systems. This was preceded by the definition of the concepts of the social network, actor, relationships. This view allows us to take into account the characteristics of the social engineering influence. In particular, the numbers of input and output arcs distinguish varieties of actors from the social engineer, user, manipulative form, vulnerability. While the importance of each of them is determined using the characteristics of centrality and prestige. At the same time, the levels of the actor, dyad, and the triad of vulnerabilities analysis of socio-technical systems to the effects of social engineering are highlighted. This will make it possible to determine the ways of such impacts taking into account the peculiarities of their realizability through user vulnerabilities and, as a result, to counteract them. In further research, it is planned to develop a method for analyzing the vulnerability of socio-technical systems to the impacts of social engineering based on the proposed model.

Keywords: socio-technical system; vulnerability analysis; social engineering; fuzzy social graph.

REFERENCES

[1] S. V. Volobuev, *Security of socio-technical systems*. Obninsk, Russia: Viking, 2012.
[2] G. A. Ostapenko, and E. A. Meshkova, *Information Operations and Attacks in Sociotechnical Systems*. Moscow, Russia: Gorjachaja linija-Telekom, 2016.
[3] A. V. Dudatyev, V. A. Luzhetsky, and D. A. Korotaev, "The method of socio-technical systems informational stability evaluation at the informational war conditions", *Eastern-European Journal of Enterprise Technologies*, vol. 2, no. 2 (80), pp. 4-11, 2016. doi: 10.15587/1729-4061.2016.65691
[4] S. I. Kravchenko, "Security of socio-technical systems", *NBI-technology*, vol. 12, no. 2, pp. 20-24, 2018. doi: 10.15688/NBIT.jvolsu.2018.2.3.
[5] D. A. Gornitska, O. G. Korchenko, and V. P. Kharchenko, "The system of sociotechnical attacks in the information environment", in *Proc. 2nd International Scientific and Practical Conference Problems of Economics and Management in Railway Transport*, Kyiv, 2007, pp. 137-138.
[6] DP "UkrNDNTs". (2016, Dec. 27). *DSTU ISO/IEC 27032. Information technology. Security techniques. Guidelines for cybersecurity (ISO/IEC 27032:2012, IDT)*. Kyiv, 2018, 50 p.
[7] 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*. Kyiv, 2017, pp. 92-98. [Online]. Available: http://ceur-ws.org/Vol-2067/paper13.pdf. Accessed on: February 12, 2020.
[8] 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: 10.20535/2411-1031.2019.7.2.190563.
[9] V. V. Mokhor, O. V. Tsurkan, and R. P. Herasymov, "Manipulative form of socio-engineering influence on the personality in cyberspace", in *Proc. Scientific and Practical Conference Actual Problems of Information Security Management of the State*, Kyiv, 2015, pp. 303-304.
[10] A. L. Tulupyev, A. E. Pashchenko, and A. A. Azarov, " Information model of the user, who may be under the threat of socioengineering attack", *Tr. SPIIRAN*, iss. 13, pp. 143-155, 2010.
[11] V. L. Buriachok, O. G. Korchenko, and L. V. Buriachok, "Social engineering as a method of information and telecommunication systems intelligence", *Zahist ìnformacìï*, vol. 14, no. 4 (57), pp. 5-12, 2012. doi: 10.18372/2410-7840.14.3471.
[12] 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: 10.18372/2225-5036.20.7308.
[13] F. Mouton, L. Leenen, and H. Venter, "Social engineering attack examples, templates and scenarios", *Computers & Security*, vol. 59, pp. 1-54, June 2016. doi: 10.1016/j.cose. 2016.03.004.
[14] 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: 10.1016/j.engappai.2018.04.009.
[15] S. Wasserman, and K. Faust, *Social Network Analysis: Methods and Applications*. Cambridge, England: Cambridge University Press, 2012. doi: 10.1017/CBO9780511815478.
[16] 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: 10.30837/IVcsitic2020201371.
[17] 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.
[18] 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.
[19] J. N. Moderson, and P. S. Nair, *Fuzzy Graphs and Fuzzy Hypergraphs*. Heidelberg, Germany: Physica-Verlag Heidelberg, 2000. doi: 10.1007/978-3-7908-1854-3.
[20] A. Kaufmann, *Introducing to the fuzzy sets theory*. Moscow, Russia: Radio i svjaz, 1982.