DOI 10.20535/2411-1031.2019.7.2.190563
УДК 004.056.53

ОКСАНА ЦУРКАН,
РОСТИСЛАВ ГЕРАСИМОВ,
ОЛЬГА КРУК

МЕТОДИ ПРОТИДІЇ ВИКОРИСТАННЮ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Проаналізовано методи протидії використанню соціальної інженерії. Як приклади їх практичного реалізування розглянуто відповідні інструментальні засоби, наприклад, Social-Engineer Toolkit, Social Engineering Defensive Framework, Social Engineering Optimizer, Kali Linux. Серед проаналізованих методів виокремлено тестування на проникнення. Цей метод протидії орієнтований на виявлення та запобігання використанню уразливостей людини (працівника, клієнта). Виявлення уразливостей людини при тестуванні на проникнення здійснюється за допомогою Social-Engineer Toolkit та Kali Linux, Cogni-Sense. Кожен зі зазначених засобів орієнтований на реалізацію загроз соціальній інженерії. При цьому Social-Engineer Toolkit може використовуватися як окремо, так і входити до складу Kali Linux. Водночас розглянуто метод підвищення обізнаності працівників, клієнтів. Для цього проводиться його навчання стосовно вірогідних сценарії атак соціальної інженерії. За результатами такого навчання удосконалюються технології і політики протидії соціоінженерному впливові. На практиці метод реалізується як Social Engineering Defensive Framework. Водночас виділено два аспекти протидії використанню соціальної інженерії: з боку суб'єкта (зловмисника), з боку об'єкта (захисника) соціоінженерного впливу. Цей метод дозволяє протидіяти використанню соціальної інженерії завдяки розгляданню вірогідних дій з боку зловмисника. При цьому вважається, що послідовність його дій визначається виключно з огляду на сценарії атак соціальної інженерії. Такий спосіб дозволяє кожній дії протиставити протидію і, я наслідок, унеможливити реалізації загроз використання соціальної інженерії. Означений метод практично реалізується інструментальним засобом Social Engineering Optimizer. Крім цього розглянуто метод виявлення і повідомлення працівниками (клієнтами) про використання соціальної інженерії. Його практичне застосування Cogni-Sense орієнтоване на інтерпретуванні людини як сенсора, що реагує на соціоінженерний вплив. Таким чином, аналіз методів протидії використанню соціальної інженерії дозволить, по-перше, врахувати їх переваги та недоліки для унеможливлення реалізації загроз соціоінженерного впливу; по-друге, розробити відповідні моделі, методи та засоби для подолання недоліків відомих рішень.

Ключові слова: соціальна інженерія, протидія використанню соціальної інженерії, метод протидії, інструментальний засіб, тестування на проникнення, обізнаність персоналу.

Постановка проблеми. Протидія використанню соціальної інженерії орієнтована на запобігання маніпулятивному впливові на свідомість (підсвідомість) людини через властиві їй уразливості. Наприклад, можна виокремити такі напрями означеної діяльності як автоматизування виявлення уразливостей людини, підвищення обізнаності персоналу, виокремлення суб'єктів і об'єктів такого впливу. Розв'язання виокремлених завдань обумовлене створенням вигаданих сюжетів і, як наслідок, сценаріїв впливання соціальних інженерів на свідомість (підсвідомість) людини. Результативність їх застосування залежить від попереднього накопичення інформації про потенційний об'єкт впливу. При цьому варто зважати на те, що загроза використання соціальної інженерії є однією з найбільш небезпечних у кіберпросторі [1]. Власне з її реалізування, зокрема [2], починалося атакування енергетичних компаній в Україні. Тому аналізування методів протидії використанню соціальної інженерії є актуальним [1] - [3].

© О. Цуркан, Р. Герасимов, О. Крук, 2019

Аналіз літературних джерел та підходів. На небезпечності загрози використання соціальної інженерії акцентовано увагу в [1], [3]. Зокрема, типові атаки, шаблони та сценарії проаналізовано в [3], [6], [7]. Тоді як дослідження методів протидії використанню соціальної інженерії виконано в [2] - [10]. Виокремлення суб'єкта та об'єкта соціоінженерного впливу здійснено в [5]. При цьому суб'єкт тлумачиться як нападник, а об'єкт – захисник. Дії нападника зведено до використання шаблонів і сценаріїв соціальної інженерії. Таке протистояння орієнтоване на прагнення нападника перемогти захисника. Крім цього, розглянуто проведення тестування на проникнення шляхом виявлення уразливостей людини [7]. Для цього рекомендовано використовувати Social-Engineer Toolkit. Цей засіб розглядається як окремий комплекс, так і як компонент Kali Linux. Використання здатності користувачів повідомляти виявляти та повідомляти про загрози використання соціальної інженерії запропоновано у [8]. Вирішення цих завдань здійснено шляхом розглядання людини як датчика безпеки (Cogni-Sense). Структуту протидії соціальній інженерії (Social Engineering Defensive Framework) розроблено в [9]. Її використання здійснюється за чотири незалежних один від одного етапи. Окрему увагу приділено підвищенню рівня обізнаності користувачів шляхом нагадування, проведення навчань [10].

Метою статті є встановлення переваг і недоліків методів протидії використанню соціальної інженерії.

Виклад основного матеріалу дослідження. У рамках соціоінженерного підходу вразливості людини тлумачяться як її слабкості, потреби, манії (пристрасті), захоплення. Маніпулювання ними дозволяє отримати несанкціонований доступ до інформації. Як наслідок, це призводить до нової моделі її поведінки, створення сприятливих умов реалізації загроз безпеці інформації і, як наслідок, зменшенню здатності систем захисту інформації протидіяти їх впливові (див., наприклад [2], рис. 1). Це відображається в таких формах як, наприклад [11], шахрайство, обман, афера, інтрига, містифікація, провокація. Використанню кожної з означених форм маніпулювання передує визначення її змісту шляхом ретельного планування, організування та контролювання [2].

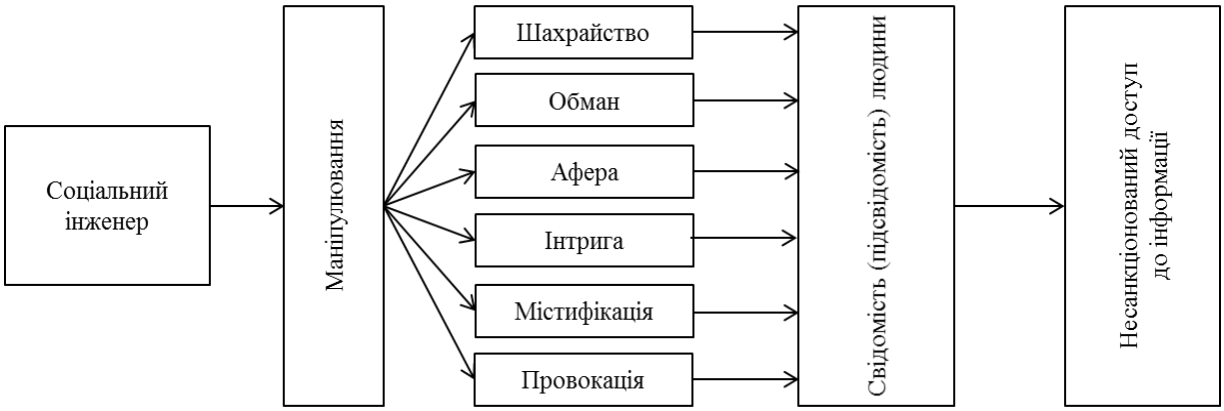

Рисунок 1 – Використання соціоінженерного підходу

З огляду на рис. 1, використання соціоінженерного підходу передбачає цілеспрямований вплив на свідомість (підсвідомість) людини проти волі, але за його згодою. Такий вплив дозволяє управляти поведінкою, наприклад, керівництва, адміністратора, користувачів через слабкості, інтереси, потреби, схильності, переконання, звички, психічний та емоційний стан. Тому маніпулювання цими уразливостями і виражається в таких формах як шахрайство, обман, афера, інтрига, містифікація, провокація. Разом з тим, використанню кожної з означених форм маніпулювання передує визначення їх сутності шляхом ретельних планування, організації та контролювання. Вони змінюються залежно від різновиду атак соціальної інженерії, а саме [11]:

Фішінг (Phishing) – масове розсилання електронної пошти великій групі адресатів. Ознайомлення з електронними листами спонукає їх до, наприклад, відкриття вкладення до

листа, переходу за посиланням на веб-сторінку. Його метою є виманювання у довірливого або неуважного персоналу комп'ютерної системи персональних даних.

Фармінг (Pharming) – перенаправлення користувачів на шахрайські сайти для отримання їх логіну та паролю. Це досягається завдяки розповсюдженню електронної пошти серед користувачів, наприклад, соціальних мереж, онлайн-банкінгу, поштових веб-сервісів.

Прітекстінг (Pretexting) – отримання інформації або спонукання до вчинення певних дій обманом на основі заздалегідь складеного сценарію або створення фіктивної ситуації. Застосовується через телефон та потребує проведення попередніх досліджень для входження в довіру.

Смішінг (Smishing) – отримання інформації шляхом масового розсилання SMS повідомлень з посиланням на веб-ресурси або з реквізитами організацій (наприклад, фінансових). Внаслідок цього здійснюються відповідні дії, наприклад, дзвінок до банку для перевірки стану рахунку з зазначенням конфіденційних даних: номеру картки, терміну дії.

Вішінг (Vishing) – отримання інформації шляхом входження в довіру під час розмови через IP-телефон. При цьому в порушення конфіденційності здійснюється завдяки викладенню прохання у повідомленні зателефонувати на певний міський номер. Наприклад, вести номер карти, паролі, PIN-коди, коди доступу або іншу інформацію.

Спір фішінг (Spear Phishing) – надсилання листа електронної пошти конкретному адресату (наприклад, керівнику, адміністраторові, користувачеві), що спонукає його до обов'язкового перегляду та відповіді на отриманий лист.

Вейлінг (Whaling) – надсилання листа електронної пошти представнику керівництва організації, що спонукає його до обов'язкового перегляду та відповіді на отриманий лист.

Так (див., наприклад [2], [11], табл. 1), отримання несанкціонованого доступу до інформації за допомогою фішингу, фармінгу, смішінгу, вішінгу, спір фішінгу, вейлінгу здійснюється шляхом використання таких форм маніпулятивного впливу як шахрайство та обман. Тоді як основою для створення фіктивних ситуацій при прітекстінгу є афера, інтрига, містифікація та провокація.

Таблиця 1 – Форми маніпулятивного впливу при соціоінженерних атаках

№ 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.	Спір фішінг	+	+	–	–	–	–
7.	Вейлінг	+	+	–	–	–	–

Тому при оцінюванні захищеності інформації в комп'ютерних системах за соціоінженерним підходом доцільно враховувати форми маніпулятивного впливу.

Методи використання соціальної інженерії направлені на імітування дій порушників проти, наприклад, персоналу організації. Вхідною інформацією для соціального інженера при спробі отримання інформації, наприклад, про комп'ютерні системи може бути контактна

інформація, що отримується з публічних джерел, наприклад: прізвища, імена, посади користувачів. За отриманою вхідною інформацію вибираються, виокремлюються вірогідні уразливості, через які можливе реалізування загроз соціальної інженерії.

Основою використання методів соціальної інженерії є [2]:

- особливості, що керують людською свідомістю;
- аудиторія або поле діяльності;
- некомпетентність аудиторії у визначених термінах і предметних областях у сфері інформаційної безпеки;
- нестійкість психологічних властивостей особистості, що характеризуються поведінковими стереотипами. Їх можна використовувати для маніпулювання через основні потреби, слабкості, бажання, ідеали.

Більшість соціальних інженерів діє за ідентичними або близькими шаблонами та, як наслідок, сценаріями атак. Тому вивчення прийомів їх "роботи" дозволяє виокремити такі рівні взаємодії з об'єктом впливу як домінування, маніпулювання, суперництво, партнерство.

Всі методи соціальної інженерії можна поділити на дві групи [2]:

1. Віддалена соціальна інженерія реалізується засобами сучасних телекомунікацій шляхом використання:

1.1. "Телефону"

Завдяки телефонії, соціальний інженер може залишатися анонімним і в той же час мати прямий зв'язок з об'єктом впливу. Останнє важливо тому, що безпосередній контакт не дає співрозмовнику часу обміркувати поведінку у вірогідних ситуаціях, зважати на всі за та проти. Вирішувати необхідно швидко, до того ж під тиском соціального інженера. Оскільки під час телефонної розмови відбувається обмін тільки звуковою інформацією, то велику роль у прийнятті рішень відіграє анотація і голос співрозмовника. Дані характеристики підбираються у відповідності з моделлю поведінки соціального інженера для отримання інформації про об'єкт впливу, наприклад:

a) начальник – людина, яка звикла віддавати команди, цінує свій час, досягає поставленої мети. Манера розмови жорстка, нетерпляча. Повна впевненість у собі і легка (або повна) зверхність до рядового персоналу. Своїм тоном показує, що проблема, з якою звернувся – дрібниця, яку необхідно вирішити якомога швидше. Ніяких прохань – тільки вимоги і вказівки. У відповідь на недовірливі або перевіряючі репліки – допустиме незадоволення і залякування співрозмовника;

b) секретар – дівчина (здебільшого) з приємним голосом. Завдання – виконати конкретне доручення начальника, не відволікаючись на умовності. Вона володіє інформацією про начальника, його справи, у своїй мові користується достовірними або недостовірними фактами, які складно перевірити. Характер розмови – м'який, з легким фліртуванням (якщо співрозмовник – чоловік). Реакція на небажання співпрацювати – бурхливе розчарування, скарга, що скаже начальство;

c) технічний співробітник – працівник організації, який характеризується поблажливим, але дружелюбним відношенням до клієнтів. Мета – усунути несправність. Супроводжується використанням специфічних термінів для відображення своєї компетентності. На відмову співпрацювати – реакція здивування, оскільки співпраця у першу чергу вигідна для клієнта. Жодних вмовлять –йому дається зрозуміти, що без його участі проблема тільки ускладнюється. Допустиме залякування тяжкими наслідками.

d) користувач – працівник, що виконує свої обов'язки і наляканий виникненням неочікуваної проблеми. Чітко виражений мотив швидкого вирішення усіх проблем і повернення до своєї рутинної роботи. Відсутність уявлення про характер проблеми, зацікавленість тільки в її вирішенні. Характер спілкування – показати безнадійність свого положення і готовність віддатися у руки спеціалісту.

1.2. Глобальної мережі Інтернет

Найбільш розповсюдженими способами реалізації методів соціальної інженерії за допомогою глобальної мережі Інтернет є:

a) проведення соціальної інженерії шляхом електронного листування;

b) проведення соціальної інженерії через системи обміну повідомленнями (Skype, Viber);

c) соціальна інженерія на форумах, чатах, блогах.

2. Особистий контакт. Найбільш складний і небезпечний метод соціальної інженерії. Крім перерахованих вимог до сценарію спілкування і моделі поведінки, соціальний інженер повинен приділяти увагу своїй зовнішності і манерам “живого” спілкування. Для правильного візуального сприйняття, необхідно правильно підібрати:

a) колір одягу та взуття;

b) манери та жести при спілкуванні;

c) положення в просторі відносно співрозмовника.

Також при використанні методів соціальної інженерії необхідно характеризувати співрозмовника. За голосом або за зовнішністю, доцільно визначити яку його слабкість доцільно використовувати для досягнення поставленої мети. До основних слабкостей людини, використання яких разом з правильно підібраною поведінкою і сценарієм розмови дозволяє досягнути очікуваного результату, належать, наприклад:

a) довірливість;

b) страх;

c) жадібність;

d) відкритість;

e) зверхність;

f) милосердя.

Основними причинами впливу на об’єкт соціальної інженерії є, наприклад:

a) відчуття достоїнства;

b) прагнення до успіху;

c) матеріальна вигода.

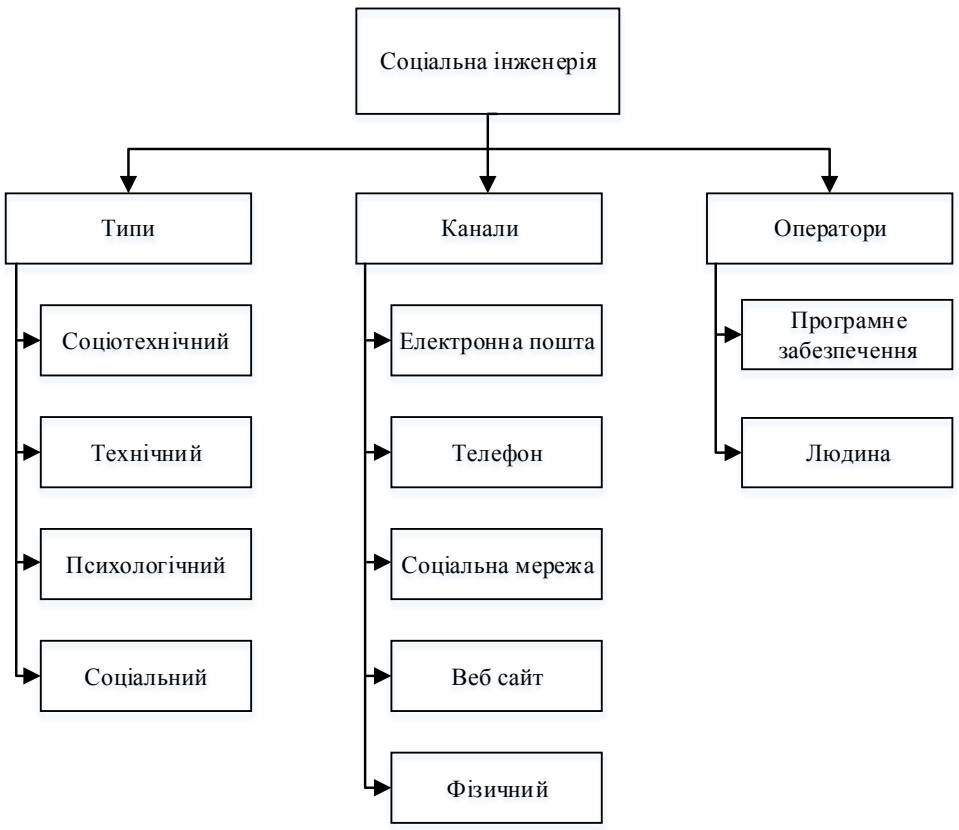

Рисунок 2 – Класифікування ознак реалізування атак соціальної інженерії

Зважаючи на сутність соціоінженерного підходу, форм маніпулятивного впливу та методів використання соціальної інженерії виокремлюються такі напрями її протидії [2], [4] – [10] як тестування на проникнення, моделювання дій об’єкта та суб’єкта соціоінженерного впливу,

Тестування на проникнення за соціоінженерними підходом орієнтоване на автоматизуванні створення і реалізування векторів атак (див., наприклад [7], рис. 3, 4). Для цього використовується інструментальний засіб соціального інженера (Social-Engineer Toolkit, SET). Він дозволяє на практиці забезпечити правдоподібність атак соціальної інженерії. Запорукою цьому є усвідомлення правильності його налаштування і, як наслідок, використання. Постачається або як окремий комплекс, або як компонент Kali Linux. При цьому можливе внесення змін до конфігураційного файлу. Це дозволяє розширювати можливості SET.

Перевагами такого методу є, по-перше, автоматизованість процесу протидії використанню соціальної інженерії; по-друге, правдоподібність векторів атак. Тоді як одним з основних недоліків є кваліфікованість користувача.

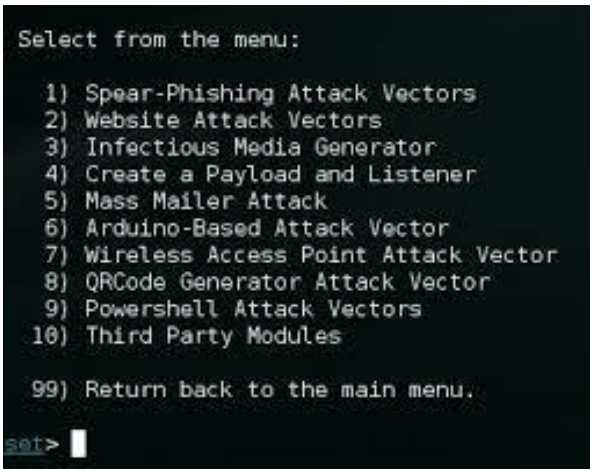

Рисунок 3 – Меню інструментального засобу SET

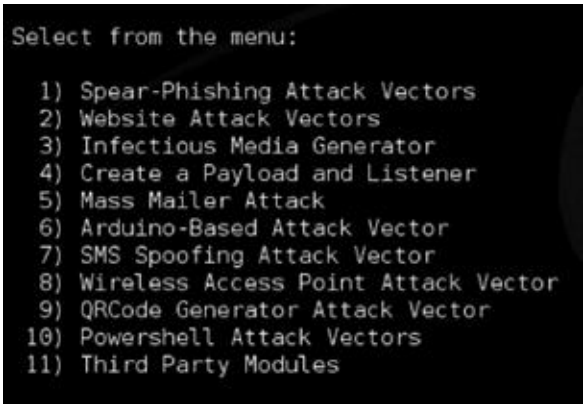

Рисунок 4 – Меню соціоінженерних атак інструментального засобу SET

Метод моделювання дій об’єкта та суб’єкта соціоінженерного впливу орієнтується на виокремлення двох ключових ролей – нападника та захисника (див., наприклад [5], рис. 5). Один з них (нападник) прагне перемогти, а інший – протидіяти соціоінженерному впливові. Наступний крок виявлення полягає у використанні соціальної інженерії від нападника до захисника. З огляду на це визначається нова позиція захисника стосовно протидії зазначеному впливові. Якщо здатність до протистояння захисника краща, ніж нападника, то їх міняють місцями за результатами порівняння між собою.

Перевагою використання даного методу є можливість виокремлення ролей як нападника, так і захисника. Проте його результативність залежить від наявних шаблонів атак соціальної інженерії. Як наслідок, можливості запобіганню їх реалізації.

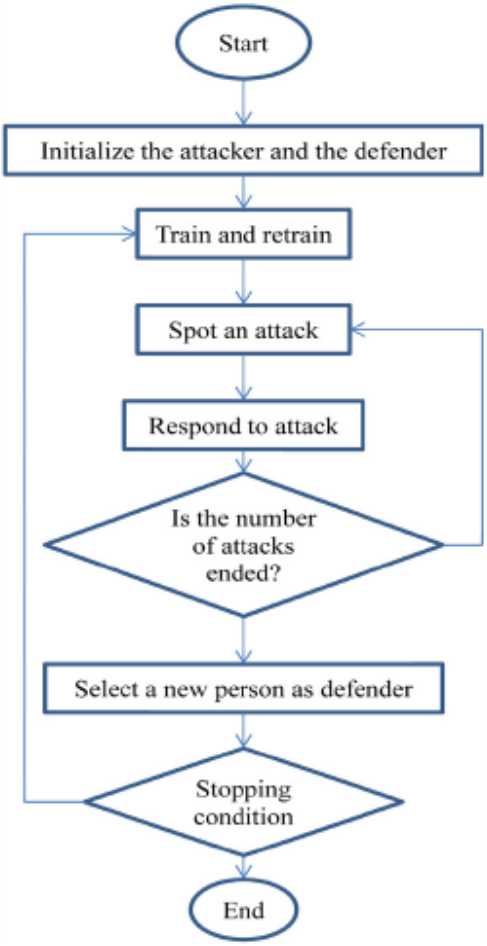

Рисунок 5 – Схема використання оптимізатора соціальної інженерії

Метод виявлення і повідомлення про атаки соціальної інженерії людиною. Цей метод практично реалізовано як інструментальний засіб Cogni-Sense. Тому для виявлення і, як наслідок, повідомлення про випадки реалізації атак соціальної інженерії достатньо тільки одного повідомлення від користувача. Такий підхід дозволяє залучати працівників організації не тільки для профілактики за допомогою, наприклад, кібергігієни, а й для активного повідомлення про загрози кібербезпеці [8].

Перевагою даного методу є залученість користувачів до активного забезпечення кібербезпеки. Водночас можливе приховування інформації про реалізування атаки соціальної інженерії окремим користувачем. Допоки об’єктом атаки не стане інший користувач.

Метод протидії використанню соціальної інженерії за SEDF (Social Engineering Defensive Framework). За основу його застосування взято такі етапи:

- визначити соціоінженерний вплив;
- оцінити можливості протидії;
- навчити персонал;
- упорядкувати існуючі технології та політику.

Перевагами методу є, по-перше, можливість адаптування з огляду на потреби організації; по-друге, незалежність етапі його застосування. Тоді як обмеженням – залежність від досвіду експерта, який залучається до навчань персоналу.

Висновки. Протидія використанню соціальної інженерії характеризується багатоаспектністю. По-перше, найбільш розповсюджений спосіб орієнтований на автоматизування виявлення уразливостей людини при тестуванні на проникнення. Тоді як, по-друге, не менш важливим є підвищення рівня обізнаності персоналу. І, по-третє, виокремлення суб'єкта та об'єкта соціоінженерного впливу для проставлення їх дій один одному.

В кінцевому випадку це дозволить врахувати типові способи використання соціальної інженерії і, як наслідок, удосконалювати та розробити методи протидії з урахуванням їх переваг і недоліків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В. Мохор, А. Богданов, и А. Килевой, *Наставления по кибербезопасности (ISO/IEC 27032:2012)*. Киев, Украина: ООО "Три-К", 2013.

[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"*. Kyiv, 2017. P. 92-98. [Online]. Available: http://ceur-ws.org/Vol-2067/paper13.pdf. Accessed on: June 11, 2019.

[3] Analysis of the Cyber Attack on the Ukrainian Power Grid. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. Accessed on: June 11, 2019.

[4] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, "Panning for gold: Automatically analyzing online social engineering attack surfaces", *Computers & Security*, vol. 69, pp. 18-34, 2017, doi: /10.1016/j.cose.2016.12.013.

[5] Fathollahi-Fard Mohammad Amir, Hajiaghaei-Keshteli Mostafa, and Tavakkoli-Moghaddam 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.

[6] F. Mouton, L. Leenen, and H. Vente, "Social engineering attack examples, templates and scenarios", Computers & Security, vol. 59, pp. 186-209, 2016, doi: 10.1016/j.cose.2016.03.004.

[7] P. Engebretson, *The Basics of Hacking and Penetration Testing. thical Hacking and Penetration Testing Made Easy*, 2013, doi: 10.1016/C2013-0-00019-9.

[8] R. Heartfield, and G. Loukas, "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework". Computers & Security, vol. 76, pp. 101–127, 2018,doi:10.1016/j.cose.2018.02.020.

[9] V. Thomas, *Building an Information Security Awareness Program*, 2014, doi:10.1016/b978-0-12-419967-5.00007-7

[10] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches", in *Proc. IEEE 4th International Conference on Future Internet of Things and Cloud*, Vienna, 2016, pp. 145-149, doi: 10.1109/FiCloud.2016.28.

[11] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks", *Journal of information security and applications*, pp. 1-10, 2014, doi: 10.1016/j.jisa.2014. 09.005.

Стаття надійшла до редакції 21.08.2019.

REFERENCE

[1] V. Mokhor, O. Bohdanov, O. Kylovyi, *Guidelines for cybersecurity (ISO/IEC 27032:2012)*. Kyiv, Ukraine: OOO "Try-K", 2013.

[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". Kyiv, 2017. P. 92-98. [Online]. Available: http://ceur-ws.org/Vol-2067/paper13.pdf. Accessed on: June 11, 2019.

[3] Analysis of the Cyber Attack on the Ukrainian Power Grid. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. Accessed on: June 11, 2019.

[4] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, "Panning for gold: Automatically analyzing online social engineering attack surfaces", *Computers & Security*, vol. 69, pp. 18-34, 2017, doi: /10.1016/j.cose.2016.12.013.

[5] Fathollahi-Fard Mohammad Amir, Hajiaghaei-Keshteli Mostafa, and Tavakkoli-Moghaddam 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.

[6] F. Mouton, L. Leenen, and H. Vente, "Social engineering attack examples, templates and scenarios", Computers & Security, vol. 59, pp. 186-209, 2016, doi: 10.1016/j.cose.2016.03.004.

[7] P. Engebretson, *The Basics of Hacking and Penetration Testing. thical Hacking and Penetration Testing Made Easy*, 2013, doi: 10.1016/C2013-0-00019-9.

[8] R. Heartfield, and G. Loukas, "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework". Computers & Security, vol. 76, pp. 101–127, 2018,doi:10.1016/j.cose.2018.02.020.

[9] V. Thomas, *Building an Information Security Awareness Program*, 2014, doi:10.1016/b978-0-12-419967-5.00007-7

[10] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches", in *Proc. IEEE 4th International Conference on Future Internet of Things and Cloud*, Vienna, 2016, pp. 145-149, doi: 10.1109/FiCloud.2016.28.

[11] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks", *Journal of information security and applications*, pp. 1-10, 2014, doi: 10.1016/j.jisa.2014. 09.005.

OKSANA TSURKAN,
ROSTYSLAV HERASYMOV,
OLHA KRUK

METHODS OF COUNTERACTING SOCIAL ENGINEERING

Methods of counteracting the use of social engineering are analyzed. Relevant tools, for example, Social-Engineer Toolkit, Social Engineering Defensive Framework, Social Engineering Optimizer, Kali Linux, have been considered as examples of their practical implementation. Among the methods analyzed, penetration testing is highlighted. This method of counteraction is focused on identifying and preventing the exploitation of human (employee, client) vulnerabilities. Human vulnerability testing for penetration testing is done using the Social-Engineer Toolkit and Kali Linux, Cogni-Sense. Each of these tools is focused on the implementation of threats to social engineering. In this case, the Social-Engineer Toolkit can be used individually or as part of Kali Linux. At the same time the method of raising awareness of employees and customers is considered. To do this, he is trained on the likely scenarios of social engineering attacks. As a result of such training, technologies and policies for counteracting socio-engineering influence are being improved. In practice, the method is implemented as the Social Engineering Defensive Framework. At the same time, there are two aspects of counteracting the use of social engineering: the subject (the attacker), the object (the protector) of socio-engineering influence. This method can counteract the use of social engineering by considering likely actions by the attacker. It is considered that the sequence of its actions is determined solely in view of the attack scenarios of social engineering. This method allows each action to counteract and, consequently, prevent the realization of threats to

the use of social engineering. This method is practically implemented by the tool Social Engineering Optimizer. In addition, the method of identifying and reporting to employees (clients) about the use of social engineering is considered. Its practical application of Cogni-Sense is focused on the interpretation of humans as a sensor that responds to socio-engineering impact. Thus, the analysis of counteracting methods for the use of social engineering will allow, first, to consider their advantages and disadvantages to prevent the realization of threats of socio-engineering influence; second, to develop appropriate models, methods and tools to overcome the shortcomings of known solutions.

Keywords: social engineering, social engineering counteracting, protection method, instrumentation, testing for penetration, staff recognition.

Цуркан Оксана Володимирівна, провідний інженер, 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.

Герасмов 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.

Tsurkan Oksana, senior engineer, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.

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

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