УДК 004.056
DOI https://doi.org/10.32782/IT/2024-3-17

Ірина СТЬОПОЧКІНА
кандидат технічних наук, доцент кафедри інформаційної безпеки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», просп. Берестейський, 37, м. Київ, Україна, 03056
***ORCID:** 0000-0002-0346-0390*
***Scopus ID:**57927656500*

Костянтин ІЛЬЇН
асистент кафедри інформаційної безпеки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», просп. Берестейський, 37, м. Київ, Україна, 03056
***ORCID:** 0009-0004-5463-0996*

Бібліографічний опис статті: Стьопочкіна, І., Ільїн, К. (2024). Профілювання користувачів для підвищення стійкості персоналу об'єктів критичної інфраструктури до кібератак, які використовують людський фактор. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 159–168, doi: https://doi.org/10.32782/IT/2024-3-17

ПРОФІЛЮВАННЯ КОРИСТУВАЧІВ ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ ПЕРСОНАЛУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДО КІБЕРАТАК, ЯКІ ВИКОРИСТОВУЮТЬ ЛЮДСЬКИЙ ФАКТОР

Робота присвячена питанням підвищення стійкості співробітників об'єктів критичної інфраструктури до кібернетичних атак, успішність яких зумовлюється використанням слабкостей людського фактору. Кожна атака соціальної інженерії, яка є запорукою успіху подальшої кібернетичної атаки, експлуатує певні риси, притаманні індивіду. Також використовуються недоліки політики безпеки, притаманні підприємству, які роблять користувачів більш вразливими.

***Метою** даної роботи є збагачення засобів підвищення стійкості персоналу об'єктів критичної інфраструктури до атак соціальної інженерії, в частині засобів діагностичного профілювання, сполучених з тренувальними функціями, які базуються на опитуванні користувачів.*

***Новизна роботи.** Запропоновано підхід до попередження атак соціальної інженерії, заснований на виявленні особливостей, які роблять користувача вразливим до таких атак. Виділено сукупність факторів, присутність яких може бути діагностовано на основі опитування, запропоновано методику опитування та відповідний програмний засіб. На основі факторів побудовано булеві функції, які можуть бути використані при визначенні приналежності користувача до відповідного профілю.*

***Методологія.** Використано експертний метод для формування опитувальника. Вразливості (фактори), які експлуатуються кібератаками на критичну інфраструктуру, визначено в результаті узагальнення існуючих напрацювань в області дослідження. Розроблене програмне забезпечення використовує опитувальник в гнучкому форматі, на основі його створюючи інтерфейс спілкування з користувачем, а на основі відповідей користувача – формуючи результат його профілювання та розбір кейсів, присутніх в опитуванні.*

***Основні результати.** Запропоноване програмне забезпечення та відповідна методика підтримують превентивні засоби та заходи безпеки підприємства, може бути використане як у якості інструменту діагностики вразливостей, так і тренувального засобу. Булеві функції, які визначають приналежність до певного профіля – можуть бути використані при побудові формалізованої моделі внутрішнього порушника.*

***Висновки.** Тестування співробітників об'єктів критичної інфраструктури за розробленою методикою дозволило виявити серед опитуваних груп користувачів, які є вразливими до атак соціальної інженерії певних видів, незважаючи на високий рівень обізнаності в інформаційних технологіях. Запропоновані в роботі засоби є допоміжними в задачах підвищення стійкості персоналу об'єктів критичної інфраструктури до кібератак з використанням людського фактора.*

***Ключові слова:** стійкість, критична інфраструктура, кібератаки, соціальна інженерія, кібербезпека.*

Iryna STOPOCHKINA
Candidate of Technical Sciences, Associate Professor at the Information Security Department, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», 37, Beresteyskyi Ave., Kyiv, Ukraine, 03056, i.stopochkina@kpi.ua
***ORCID:** 0000-0002-0346-0390*
***Scopus ID:** 57927656500*

Kostiantyn ILIN
Assistant at the Information Security Department, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», 37, Beresteyskyi Ave., Kyiv, Ukraine, 03056, kostya.ilin_ipt@lll.kpi.ua
***ORCID:** 0009-0004-5463-0996*

To cite this article: Styopochkina I., Ilyin K. (2024). User profiling to increase the resilience of critical infrastructure personnel to cyberattacks that use the human factor. Information Technology: Computer Science, Software Engineering and Cyber Security, 3, 159–168, doi: https://doi.org/10.32782/IT/2024-3-17

USER PROFILING TO INCREASE RESILIENCE OF CRITICAL INFRASTRUCTURE PERSONNEL TO CYBER ATTACKS USING THE HUMAN FACTOR

The work is devoted to issues of increasing the resistance of employees of critical infrastructure objects to cybernetic attacks, the success of which is determined by the use of human factor weaknesses. Each social engineering attack, which is usually the key to the success of a subsequent cyber attack, exploits certain traits inherent in the individual. It also exploits flaws in enterprise-specific security policies that make users more vulnerable.

***The purpose** of this work is to enrich the means of increasing the resistance of personnel of critical infrastructure objects to social engineering attacks, in terms of diagnostic profiling tools combined with training functions based on user surveys.*

***The novelty of the work**. An approach to the prevention of social engineering attacks is proposed, based on the identification of features that make the user vulnerable to such attacks. A set of factors, the presence of which can be diagnosed on the basis of a survey, is identified, a methodology and a corresponding software tool are proposed. Based on the factors, Boolean functions have been built that can be used to determine whether the user belongs to the appropriate profile.*

***Methodology.** An expert method was used to form the questionnaire. Vulnerabilities (factors) that are exploited by cyberattacks on critical infrastructure are determined as a result of the generalization of existing developments in the field of research. The developed software uses the questionnaire in a flexible format, based on it creating a communication interface with the user, and based on the user's answers, forming the result of his profiling and analyzing the cases present in the survey.*

***Main results**. The proposed software and the corresponding methodology support preventive measures and security measures of the enterprise, can be used both as a tool for diagnosing vulnerabilities and as a training tool. Boolean functions that determine belonging to a certain profile can be used when building a formalized model of an internal violator.*

***Conclusions**. Testing of employees of critical infrastructure facilities according to the developed methodology made it possible to identify among the interviewed groups of users who are vulnerable to social engineering attacks of certain types, despite a high level of knowledge in information technologies. The tools proposed in the work are helpful in the tasks of increasing the resistance of personnel of critical infrastructure objects to cyber attacks using the human factor.*

***Key words:** resilience, critical infrastructure, cyber attacks, social engineering, cybersecurity.*

Актуальність задачі. Незважаючи на наявність великої кількості засобів та тренінгів із питань протидії соціальній інженерії, більше 50% успішних кібернетичних атак засновані саме на експлуатації людського фактора. Наразі значна кількість об'єктів критичної інфраструктури потерпає від атак соціальної інженерії, які є першим етапом для подальшого виконання зловмисних кібервпливів. Кількість таких атак лише підвищилась у воєнний час, таким чином, існуючі засоби протидії атакам з використанням людського фактора потребують збагачення та адаптації до особливостей об'єктів критичної інфраструктури. Зростання кількості та різноманітності успішних атак соціальної інженерії показує, що тренування реагування на конкретні приклади атак соціальної інженерії є лише частиною проблеми, інша частина полягає у причинах, чому працівник є вразливим до тих чи інших атак. Виявлення цих причин, або ж організаційних та соціальних факторів, систематизація їх ролі в експлуатації в ході кібератак є предметом даної роботи. Супутньою задачею є розробка тренінгового засобу, який можна гнучко модифікувати під потреби конкретного об'єкта критичної інфраструктури.

Аналіз досліджень та публікацій. Питання виявлення вразливостей користувача до атак соціальної інженерії розглядалось в попередніх роботах. Зокрема, (Cofense, 2024), в якому емулюються ситуації обходу SEG (Security Email Gateway). Недоліком цього рішення є те, що воно не враховує специфіку конкретного підприємства, не кастомізується, та переважно орієнтоване лише на атаки вектором пошти. Ресурс (Knowbe4, 2024) пропонує широкий спектр тренувань, які дозволяють виявити рівень обізнаності в області кібербезпеки користувачів,

провести симуляцію фішингових атак та надати кейси для опрацювання. Також, слід відзначити складність чи неможливість кастомізації запропонованих кейсів під потреби підприємства, і зосередженість переважно на фішингових атаках, залишаючи поза увагою інші способи соціальної інженерії. Інструменти (Barracuda Networks, 2019) мають схожі особливості та недоліки із вищезазначеними тренінговими засобами та відрізняється складністю використання. Сервіс (DataArt, 2024) надає засіб тестування шляхом емуляції реальних ситуацій для користувачів підприємства, проводячи тестування на проникнення з використанням соціальної інженерії. Такі засоби скоріше слугують для зрізу стану безпеки підприємства, ніж навчанню користувачів. Відповідно, подібні засоби мають під собою алгоритмічне наповнення, яке використовує дослідження актуальних кібератак з використанням людського фактора (Mataracioglu, 2011). Інші загальні ідеї анкетувань користувачів для покращення їх стійкості до атак соціальної інженерії надано в (Gamagedara Arachchilagea, 2014).

Спільною рисою вказаних та багатьох інших робіт та засобів є те, що вони спрямовані на навчання та/ або тестування користувачів на конкретних випадках атак соціальної інженерії, які досить швидко застарівають. Разом з цим, причина успішності відповідних атак, яка полягає у вразливості користувача, що не завжди пов’язана з його необізнаністю, залишається поза увагою. В даній роботі пропонується діагностичний засіб, який сполучений із принципом роботи тренінгового засобу. Запропоновано перелік соціальних та психологічних якостей особи, які роблять особистість вразливою до ряду атак соціальної інженерії. Запропоновано булеві функції для виявлення сукупності рис (профілів), які визначають підвищену вразливість користувача до пропозицій соціального інженера.

Дослідження людських особливостей, які роблять людину вразливою до атак соціальної інженерії, розпочато в роботах (Hadnagy, 2018; Mouton, 2016; Bhakta, 2015). Зокрема, робота (Bhakta, 2015) дає уявлення про побудову таксономії соціо-інженерних атак та їх зв’язок із факторами, які експлуатуються. В роботі (Shevchenko, 2022) розглянуто приклади популярних атак соціальної інженерії під час військового стану в Україні, що дає розуміння людських слабкостей, які експлуатуються.

Деякі із цих особливостей можна ліквідувати заздалегідь, безвідносно до типу атак, які можуть бути застосовані. Наприклад, вразливість користувача до ситуацій, які використовують страх перед керівництвом, або ж невміння відмовляти у незручному становищі, або ж надмірну довірливість. Опитувальний лист складається таким чином, щоби виявити насамперед такі вразливості, і, супутньо, пояснити опитуваному кейси, на яких базуються відповідні питання, у форматі тренінга. Концепт опитування та відповідного програмного засобу автори роботи представили в (Кузьмін, 2024), в даній роботі представлено розширений та поглиблений результат дослідження.

Супутньо, шляхом опитування виявляються недоліки політики безпеки підприємства критичної інфраструктури, які потенційно наражають на небезпеку в виді кібератак, які експлуатують людський фактор, приклади яких наведено в (Lee, 2016; Zetter, 2014; Gallagher, 2016; Liptak, 2016; Sanger, 2021; Tidy, 2021). Зокрема, в роботі (Lee, 2016) проаналізовано етапи кібер-атаки на українську енергетичну систему, в роботі (Zetter, 2014) надано інформацію по атаці на іранський ядерний об’єкт, в публікаціях (Gallagher, 2016; Liptak, 2016) висвітлено особливості атак на транспортну систему Сан-Франциско, в (Sanger, 2021; Tidy, 2021) надано факти по кібератаці на нафтопереробну систему Сполучених Штатів. Ці аналітичні роботи свідчать про вдале використання людського фактору та недоліки політики безпеки, що є запорукою успіху подальшої кібератаки.

Супутньою розв’язаною задачею даної роботи є виявлення ряду характеристик користувача, на які слід звертати увагу для запобіганню інсайдерства.

Нелояльність до компанії, корисливість, агресивність та інші ознаки – можуть слугувати індикаторами потенційно небезпечної ситуації. Перелік таких ознак, опис відповідних профілів та методику їх виявлення запропоновано в даній роботі.

Для виявлення подібних ознак пропонується використовувати підходи соціологічних досліджень, та уже сформовані опитувальні засоби, які пропонуються в роботах (Merecz, 2009; Andersen, 2002; Kersten, 2024; Vo, 2022; Bustamante, 2014; Test Partnership, 2023; Personal Work-Related Responsibility Test, 2016). Зокрема, роботи (Merecz, 2009; Andersen, 2002; Kersten, 2024) присвячені виявленню рівня агресивності, робота (Vo, 2022) розглядає питання вмотивованості на робочому місці, в роботі (Bustamante, 2014) розглянуті питання тестування працелюбності, звіт (Test Partnership, 2023) демонструє приклад комплексного тестування працівника по кількох напрямках,

звіт (PE Konsult Ltd., 2016) надає тест на відповідальність працівника. Засіб тестування (Parvez, 2024) спрямований на виявлення рівня корисливості. Особливості використання людського фактору при атаках на об'єкти критичної інфраструктури можна знайти в (Ghafir, 2018). Дослідження, пов'язані із виділенням людських характеристик, що сприяють соціальній інженерії, були здійснені в роботах (Krombholtz, 2013; Kronberg, 2015).

Мета роботи. Метою роботи є збагачення засобів підвищення стійкості персоналу об'єктів критичної інфраструктури до атак соціальної інженерії, в частині засобів профілювання, сполучених з тренувальними функціями, які базуються на опитуванні користувачів.

Виклад основного матеріалу.

Виділення сукупності вразливостей користувача. Виділимо характеристики користувача, які можуть сигналізувати про схильність до впливів соціальної інженерії.

Виділимо особистісні фактори, які можуть бути тригерами для різних атак соціальної інженерії: схильність до страхів, боязкість F; невміння відмовляти R; невміння обмежуватись при одержанні чогось (жадібність, в тому числі до роботи, азартність в іграх тощо) B; необережність A; необізнаність P; схильність до ліні чи прокрастинації L; байдужість I; непунктуальність U. В залежності від комбінації факторів можна виділити типові профілі осіб, які є схильними до певних атак соціальної інженерії. Кожен профіль визначається відповідною булевою функцією:

1) $P1 = F \cap R \cap I$, профіль, який відповідає м'якій людині, якою легко маніпулювати. Якщо вона навіть помітить порушення, простіше буде промовчати про це.

2) $P2 = B \cap L \cap P$ – профіль, який відповідає активній людині, яка прагне одержати різноманітні блага. Однак, схильна до лінощів, та не цікавиться можливими наслідками рішень. Це дозволяє соціальному інженеру пропонувати варіанти легкої наживи, та порушень кібербезпеки.

3) $P3 = A \cap I \cap U$ – профіль, який відповідає необережній людині, яка не є пунктуальною та уважною. Необізнаність підсилює вразливість до атак, які розраховані на імпульсивні, необдумані рішення.

4) $P4 = I \cap B \cap A$ – профіль, який відповідає людині, схильній до ризику, і достатньо байдужій до негативних наслідків власних дій.

В анкеті пропонуються питання, які відповідають факторам {F, R, B, A, P, L, I, P} чи їх комбінації. Вважається, що фактор присутній, і відповідна булева змінна істинна, коли опитування показало перевищення значення числової оцінки даного фактора над середнім по групі. Або, в цілях тренування, можна перевірити наявність у особи деяких із вказаних властивостей, які частіше експлуатуються соціальними інженерами.

З точки зору аналізу співробітника об'єкту критичної інфраструктури, який має доступ до критичної інформації та/або функцій системи, найбільш небезпечними особистісними факторами є: {A, P, I, U}. Вони можуть сигналізувати про невміння, чи небажання усвідомлювати важливість роботи, прийняття рішень, що є неприпустимим для співробітника об'єкта критичної інфраструктури індустріального типу.

Питання анкети, які містяться в опитувальнику соціотехнічного спрямування, спрямовані на виявлення розуміння співробітником політики безпеки підприємства, наявності чітких інструкцій та обмежень щодо небезпечних дій, та впровадження відповідних технічних засобів та організаційних заходів. Так само, питання анкети можуть згруповані по факторах, до яких в певних ситуаціях чутлива будь-яка людина: сильний вплив (F1), взаємність (F2), перевантаження (F3), недостача (F4), оманливі відносини (F5), терміновість (F6), соціальне схвалення (F7).

Ми можемо розрахувати $Q\left(\{F_i\}\right)$ – сумарний бал по одному чи кількох факторах. Кожна атака соціальної інженерії має свій паттерн, який використовує той чи інший фактор. Наприклад, вішинг часто експлуатує фактори F1, F3, F6. Претекстінг через месенджер використовує фактори F4, F5. Так само, різні види фішингових атак можуть використовувати F7, F2 або інші фактори.

В анкеті питання згруповані також по середовищах- векторах здіснення атаки. Виділено: фізичне середовище, електронну пошту, месенджер, веб-ресурси, соціальні мережі, телефон, особисте спілкування.

Застосунок для діагностування та тренінгів. Питання, варіанти відповідей до них та бали представлені у структурованому вигляді в форматі json. Парсер зчитує питання, і представляє їх та варіанти відповідей у користувацькому інтерфейсі.

Результати опитування узагальнюються у вигляді профілю, який побудований в вигляді «рози вітрів», в якості напрямків виділяються особистісні вразливості та вразливості загального виду (рис. 1). За описаною в питанні ситуацією наводиться пояснення для досягнення навчального ефекту. Опитування також

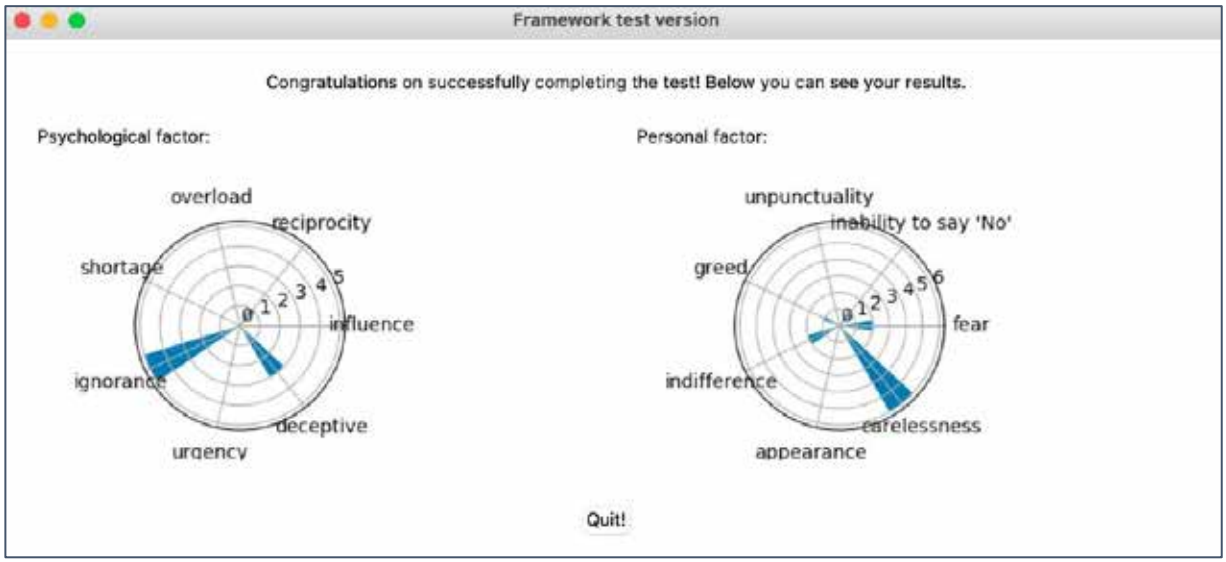

Рис. 1. Приклад візуалізації профілю користувача, який пройшов тестування

Таблиця 1

Результати опитування

Соціальні техніки		Соціо-фізичні		Соціо-технічні	
Враховані фактори	**Відсоток вразливих**	**Враховані фактори**	**Відсоток вразливих**	**Враховані фактори**	**Відсоток вразливих**
F,F1	40	F,F1	20	F7	30
R, F2	10	R,F2	30	B,F4	0
B,F4	60	U,F3	50	A,F2	20
A,F5	20	B,F4	20	P,A	20
P,F4	10	A,P,F4	60	A,F7	30
L,P,F6	0	P,I	40	F,F6	30
F,F6	0	F,F6	40	F,P	10
R	0	F5	60	P	0

дозволяє виявити певні недоліки організаційно-технічного характеру, які притаманні об'єкту критичної інфраструктури на якому здійснюється опитування. Зокрема, можна виявити відсутність заборон на встановлення стороннього програмного забезпечення, використання сторонніх носіїв, відсутність чітких режимно – перепускних правил, незахищений документообіг, незахищене ділове спілкування тощо. За запропонованою методикою було здійснено опитування працівників компаній, що віднесені до критичної інфраструктури, група дослідження складалась із 10 персон, обраних випадковим чином, високого рівня обізнаності в інформаційних технологіях (табл. 1). Основна мета експерименту – оцінити складність запропонованого опитувальника для обізнаного користувача, зручність його використання, та проілюструвати працездатність запропонованого програмного та інформаційного забезпечення діагностування. За відгуками респондентів, опитувальник не повинен бути надто довгим, оскільки увага опитуваного розсіюється, водночас, мала кількість питань може бути недостатньою для виявлення потенційної проблеми. Даний опитувальник було складено з 30 кейсів, по 10 ситуаційних питань на атаки, які ведуться через соціальне, соціо-технічне та соціо-фізичне середовище та можуть бути точкою входу для подальшої кібератаки.

За проведеним опитуванням було виявлено недоліки політики безпеки в організаціях, до яких належали опитувані, зокрема, стосовно використання месенджерів: 80%; документообігу: 30%; веб ресурсів: 90%; телефонії: 70%. Це потенційно наражає на небезпеку персонал, який працює з цими ресурсами.

Проблема інсайдерства та порушень кібербезпеки. За допомогою опитувань можна виявляти ознаки, які є потенційними тригерами здійснення порушень політики безпеки, що особливо важливо для об'єктів критичної інфраструктури. Одержану інформацію можна використовувати на етапі побудови моделі

порушника. Виділимо такі ознаки: відповідальність – V, корисливість – К, агресивність – А, працелюбність – Р, мотивація – М. При побудові профіля користувача можна використовувати функцію $f = f(V,K,A,P,M)$.

Складемо булеві функції f_i, за допомогою яких можна виділити потенційно вразливих з точки зору внутрішніх порушень працівників:

1) Незадоволений працівник, з ознаками агресії:

$$f_1 = (V \cup \neg V) \cap (K \cup \neg K) \cap A \cap (\neg M) \cap (P \cup \neg P);$$

2) Безвідповідальний та невмотивований працівник, потенційне джерело ненавмисних порушень безпеки:

$$f_2 = (\neg V) \cap (K \cup \neg K) \cap (A \cup \neg A) \cap (P \cup \neg P) \cap (\neg M),$$

3) Корисливий працівник $f_3 = (V \cup \neg V) \cap (K) \cap (A \cup \neg A) \cap (M \cup \neg M) \cap (P \cup \neg P)$; і його небезпечний підтип – корисливий, агресивний та невмотивований працівник, здатний на свідомі порушення безпеки: $F_1 = f_4 = (V \cup \neg V) \cap (K) \cap (A) \cap (\neg M) \cap (P \cup \neg P)$.

Вважаємо змінну булевої функції істинною, якщо її значення є вищим за середній рівень по групі.

Рівень комп'ютерної досвідченості персоналу та визначення схильності до порушень кібербезпеки визначають, який тип кіберпорушення може скоїти респондент та на якому саме рівні інформаційної системи.

Таким чином, модель порушника з урахуванням запропонованого підходу може включати такі ознаки:

– Тип порушника: 1)внутрішній (класифікація згідно запропонованого профілю, з виділенням рис V,K,A,M,P), 2)зовнішній (хакер, кіберкримінал, хактивіст, злочинне угруповування);

– Права по відношенню до системи (згідно розподілу прав доступу);

– Рівень кваліфікації (для внутрішніх – згідно тесту на знання інформаційно-комунікаційних технологій, обійманої посади). Цей рівень зазвичай визначається на технічній співбесіді при наймі працівників.

Для ілюстрації було проведено опитування 35 респондентів по 100 бальній шкалі, яке дозволило виявити відповідні риси (рис. 2-6). В якості опитуваних обрано співробітників колективу, які за посадовими обов'язками часто взаємодіють із сторонніми особами, і є потенційною «точкою входу» до інформаційної системи компанії.

Обчислено коефіцієнт кореляції для виявлення зв'язку між парами ознак по групі (табл. 3).

В досліджуваній групі відсутні представники профіля 1) (агресивний та невмотивований працівник), однак, є значна кількість осіб,

Рис. 2. Рівень корисливості респондентів 1-35

Рис. 3 Рівень відповідальності респондентів 1-35

Рис. 4. Рівень працелюбності респондентів 1-35

Рис. 5. Рівень вмотивованості респондентів 1-35

Рис. 6. Рівень агресивності респондентів 1-35

які відповідають типажу 2) – невмотивований та безвідповідальний, який може бути джерелом ненавмисних порушень безпеки, в тому числі і легкою жертвою соціального інженера. Істотна кількість працівників з підвищеним рівнем корисливості теж свідчить про потенційну небезпеку атак з використанням людського фактора.

Методика проведення опитування.

Методика для швидкого опитування на виявлення ознак потенційних вразливостей до атак соціальної інженерії складається з наступних кроків:

1) Опитуваний має бути попереджений про ціль опитування. Ціллю є не перевірка рівня знань чи навичок опитуваного, а виявлення того, які дії насправді можливі в умовах, де працює опитуваний, та варіанти його поведінки.

2) Кожен опитуваний незалежно проходить тестування з використанням програмного забезпечення, відмічаючи ті відповіді, які найбільше для нього підходять.

3) Використання сторонніх джерел при анкетуванні заборонене, відповіді на питання не потребують спеціальних знань. Час опитування має бути достатнім, щоб прочитати всі питання та зрозуміти їхню суть.

4) Для досягнення навчального ефекту, всі кейси, які пропонуються в опитувальнику та коментарі, надані програмою у відповідь, варто додатково розібрати та прокоментувати. Коментарі може надати штатний фахівець з кібербезпеки.

5) Програмне забезпечення за результатами опитування формує «профіль» опитуваного, відмічаючи його слабкі та сильні сторони. Чим вищий бал одержано користувачем по якомусь фактору, тим сильніше проявляється проблема в цьому напрямку. Сукупності особистісних та загально-людських факторів можуть утворювати комбінації, які небезпечні з точки зору вразливості до атак соціальної інженерії. Зокрема, це профілі $P1-P4$.

6) Фахівець з кібербезпеки за участю спеціаліста по людських ресурсах (HR) та, можливо, штатного психолога організації роблять висновки щодо необхідності проведення превентивної та коригуючої роботи стосовно виявлених вразливостей.

Опитування, яке може виявити схильності працівника до скоєння потенційних внутрішніх порушень політики безпеки, здійснюється із залученням штатного спеціаліста з проведення опитувань, за допомогою загальновідомих опитувальників на виявлення ознак корисливості, відповідальності (та безвідповідальності), вмотивованості (та невмотивованості), працелюбності (та ліні), агресивності. Завдяки опитуванню можна виявити ознаки, притаманні профілям $f_1 - f_4$. Булева змінна, яка входить до

Таблиця 2

Характеристики опитування по ознаках

Ознаки	Середнє	Відхил	Дисперсія
Відповідальність	32,5	10,2	104,8
Корисливість	27,0	10,2	104,7
Працелюбність	23,1	8,6	74,9
Мотивація	30,9	9,9	99,0
Агресивність	25,0	10,1	103,6

Таблиця 3

Коефіцієнти кореляції для пар ознак

Ознаки	Коефіцієнт кореляції
Корисливість, агресивність	0,79
Безвідповідальність, непрацелюбність	0,75
Невмотивованість, агресивність	-0,71
Невмотивованість, непрацелюбність	0,68
Невмотивованість, безвідповідальність	0,78

функції профіля, приймає значення «Істина», якщо результат респондента перевищує середнє по групі. Одержані результати можуть бути прийняті до відома при призначенні респондентів на відповідальні посади на об'єкті критичної інфраструктури.

Висновки. Опитування, проведене із використанням запропонованих у роботі методики та засобів, показало, що респонденти правильно реагують на шаблонні ситуації, однак, у випадку ситуацій, які містять елементи форс-мажору, оманливих відносин, чи одержання вигоди можуть несвідомо діяти за задумом соціального інженера. Таким чином, організації повинні приділити увагу тренінгам, які зачіпають саме такі, нестандартні ситуації, які можуть виникнути на об'єкті критичної інфраструктури.

Для запобігання цим атакам треба не лише тренувати персонал на стійкість до поширених атак соціальної інженерії, але й ліквідувати наявні людські вразливості. Робота над вразливостями персоналу може проводитись як із залученням психологів, так і шляхом організаційних заходів: підтримки доброзичливої атмосфери в колективі, підвищенні вмотивованості працівників, впровадження прозорих механізмів комунікації. Важливим є впровадження засобів та заходів політики безпеки.

Запропоновані в роботі профілі та методика не є підставою для остаточних суджень, вони лише є допоміжним діагностичним інструментом для попередження кібератак із використанням слабкостей людського фактора.

Перспективою подальших досліджень може бути розробка графа знань, для швидкого пошуку та ідентифікації відповідних вразливостей у взаємозв'язку із техніками соціальної інженерії.

Подяки. Автори висловлюють подяку Глібу Кузьміну, та Юлії Голубничій, випускникам НН ФТІ КПІ ім. Ігоря Сікорського, за допомогу в постановці практичних експериментів. Всі дослідження здійснювались із дотриманням вимог Закону України «Про захист персональних даних».

ЛІТЕРАТУРА:

1. Cofense. Phishing security awareness training. 2024. URL: https://cofense.com/

2. Knowbe4. New-School Security Awareness Training. 2024. URL: https://www.knowbe4.com/

3. Barracuda Networks. Barracuda Phishline. 2019. URL: https://assets.barracuda.com/assets/docs/dms/Barracuda_PhishLine_DS_US.pdf

4. DataArt. Social Engineering Test. 2024. URL:https://www.dataart.com/services/security/social-engineering-test

5. T. Mataracioglu, S. Ozkan. 2011. User awareness measurement for phishing attacks. Information Management & Computer Security, 19(4), 315-327. URL: arXiv:1108.2149

6. N. A. Gamagedara Arachchilagea, S. Love. Security awareness of computer users: A phishing threat avoidance perspective. 2014. DOI:10.1016/j.chb.2014.05.046

7. C. Hadnagy. The Science of Human Hacking. John Wiley & Sons, Inc., Indianapolis, USA. 2018.

8. F. Mouton, L. Leenen, & H. S. Venter. Social engineering attack framework*. Proceedings of the South African Institute of Computer Scientists and Information Technologists Conference.* ACM, New York, NY, USA. 2016. DOI:10.1109/ISSA.2014.6950510

9. P. Bhakta, M. A. Harris. Semantic analysis of dialogs to detect social engineering attacks. 2015. *DOI:10.1109/ICOSC.2015.7050843*

10. Shevchenko G., Stopochkina I., Babenko I., Peculiarities of phishing threats and preventive measures in the conditions of war in Ukraine // Theoretical and Applied Cybersecurity, Vol. 4 No. 1. 2022. https://doi.org/10.20535/tacs.2664-29132022.1.

11. Г. І. Кузьмін, І. В. Стьопочкіна, К. І. Ільїн. Розробка фреймворка для тестування співробітників критичної інфраструктури на вразливості до атаксоціальної інженерії. Матеріали Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», 13-17 травня 2024, м. Київ. С. 147–150. URL: conf.ipt.kpi.ua.

12. R. M. Lee, M. J. Assante, T. Conway. Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Industrial Control Systems. 2016. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

13. K. Zetter. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group. 2014. 433 p.

14. S. Gallagher. Ransomware locks up San Francisco public transportation ticket machines. Ars Technica. 2016. URL: https://arstechnica.com/information-technology/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack/

15. A. Liptak. Hackers are holding San Francisco's light-rail system for ransom. *The Verge*. 2016. URL: https://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware-cybersecurity-muni

16. D.E. Sanger, C. Krauss, N. Perlroth. Cyberattack Forces a Shutdown of a Top U.S. Pipeline. *The New York Times.* 2021. https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

17. J. Tidy. Colonial hack: How did cyber-attackers shut off pipeline? *BBC News*. 2021. https://www.bbc.com/news/technology-57063636

18. D. Merecz, M. Drabek, A. Mościcka-Teske. Aggression at the workplace – psychological consequences of abusive ecounter with coworkers and clients. International journal of occupational medicine and environmental health. 2009. № 22. P.243–260. DOI:10.2478/v10001-009-0027-2.

19. C.A.Andersen, B.J.Bushman. Human aggression. 2002. DOI:10.1146/annurev.psych.53.100901.135231

20. R. Kersten, T. Greitemeyer. Human aggression in everyday life: An empirical test of the general aggression model. 2024. https://doi.org/10.1111/bjso.12718

21. T.-T-D. Vo, C. Chen, K. Tuliao. Work Motivation: The Roles of Individual Needs and Social Conditions. Behavioral Sciences. 2022. 12(2):49. DOI: 10.3390/bs12020049

22. E. E. Bustamante, C. L. Davis, D. X. Marquez. A Test of Learned Industriousness in the Physical Activity Domain. 2014. DOI:10.5539/ijps.v6n4p12

23. Test Partnership. Simone Sample. 2023. TPAQ-45 Complete Profile. Full Report. URL: https://www.testpartnership.com/samplereports/sample-report-personality.pdf

24. PE Konsult Ltd. Personal Work-Related Responsibility Test (WRT). 2016. URL: https://www.pekonsult.ee/testid/Vastutus.pdf

25. H. Parvez. 'Am I selfish?' Quiz (Selfishness score). 2024. URL: https://www.psychmechanics.com/am-i-selfish-quiz/

26. I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour et al. Security threats to critical infrastructure: the human factor. 2018. DOI:10.1007/s11227-018-2337-2

27. K. Krombholtz. Social Engineering Attacks on the Knowledge Worker. Proceedings of the 6th International Conference on Security of Information and Networks. 2013. URL: https://publications.sba-research.org/publications/sig-alternate.pdf

28. B. Kronberg, J. Swanlund, H. Jeppsson. Social Engineering. A study in awareness and measures. 2015. URL: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=5474076&fileOId=5474079

REFERENCES:

1. Cofense. Phishing security awareness training. 2024. Retrieved from: https://cofense.com/

2. Knowbe4. New-School Security Awareness Training. 2024. Retrieved from: https://www.knowbe4.com/

3. Barracuda Networks. Barracuda Phishline. 2019. Retrieved from: https://assets.barracuda.com/assets/docs/dms/Barracuda_PhishLine_DS_US.pdf

4. DataArt. Social Engineering Test. 2024. Retrieved from:https://www.dataart.com/services/security/social-engineering-test

5. Mataracioglu, T., Ozkan, S. (2011). User awareness measurement for phishing attacks. *Information Management & Computer Security*, 19(4), 315–327. Retrieved from: arXiv:1108.2149

6. N. A. Gamagedara Arachchilagea, S. (2014). Love. Security awareness of computer users: A phishing threat avoidance perspective. DOI:10.1016/j.chb.2014.05.046

7. Hadnagy, C. (2018). The Science of Human Hacking. John Wiley & Sons, Inc., Indianapolis, USA.

8. Mouton, F., Leenen, L. & Venter, H. S. (2016). Social engineering attack framework. *Proceedings of the South African Institute of Computer Scientists and Information Technologists Conference*. ACM, New York, NY, USA. DOI:10.1109/ISSA.2014.6950510

9. Bhakta, P. & Harris, M. A. (2015). Semantic analysis of dialogs to detect social engineering attacks. *DOI:10.1109/ICOSC.2015.7050843*

10. Shevchenko, G, Stopochkina, I., Babenko, I. (2022). Peculiarities of phishing threats and preventive measures in the conditions of war in Ukraine. Theoretical and Applied Cybersecurity, Vol. 4 No. 1. DOI: https://doi.org/10.20535/tacs.2664-29132022.1.

11. G. Kuzmin, I. Stopochkina, K. Ilin. Development of framework for critical indfrastructure employee testing on social engineering vulnerabilities (in Ukrainian). Materials of All-Ukr. Scient. and Pract. Conference «Theoretical and applied problems of physics, mathematics and infromatics», 13-17th of May. 2024, Kyiv. P. 147–150.

12. Lee, R. M., Assante, M. J., Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Industrial Control Systems. Retrieved from: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

13. Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group. 433 p.

14. Gallagher, S. Ransomware locks up San Francisco public transportation ticket machines. Ars Technica. Retrieved from: https://arstechnica.com/information-technology/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack/

15. Liptak, A. (2016). Hackers are holding San Francisco's light-rail system for ransom. *The Verge*. Retrieved from: https://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware-cybersecurity-muni

16. Sanger, D. E., Krauss, C., Perlroth, N. (2021). Cyberattack Forces a Shutdown of a Top U.S. Pipeline. *The New York Times.* https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

17. Tidy. J. (2021). Colonial hack: How did cyber-attackers shut off pipeline? *BBC News*. https://www.bbc.com/news/technology-57063636

18. Merecz, D., Drabek, M., Mościcka-Teske, A. (2009). Aggression at the workplace – psychological consequences of abusive ecounter with coworkers and clients. *International journal of occupational medicine and environmental health*. № 22. P.243–260. DOI:10.2478/v10001-009-0027-2.

19. Andersen, C. A., Bushman, B. J. (2002). Human aggression. DOI:10.1146/annurev.psych.53.100901.135231

20. Kersten, R., Greitemeyer, T. (2024). Human aggression in everyday life: An empirical test of the general aggression model. https://doi.org/10.1111/bjso.12718

21. T.-T-D.Vo, Chen, C., Tuliao, K. (2022). Work Motivation: The Roles of Individual Needs and Social Conditions. Behavioral Sciences. 12(2):49. DOI: 10.3390/bs12020049

22. Bustamante, E. E., Davis, C. L., Marquez, D. X. (2014). A Test of Learned Industriousness in the Physical Activity Domain. DOI:10.5539/ijps.v6n4p12

23. Test Partnership. Simone Sample. TPAQ-45 Complete Profile. Full Report. 2023. Retrieved from: https://www.testpartnership.com/samplereports/sample-report-personality.pdf

24. PE Konsult Ltd. Personal Work-Related Responsibility Test (WRT). 2016. Retrieved from: https://www.pekonsult.ee/testid/Vastutus.pdf

25. Parvez, H. (2024). 'Am I selfish?' Quiz (Selfishness score). Retrieved from: https://www.psychmechanics.com/am-i-selfish-quiz/

26. Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H. et al. (2018). Security threats to critical infrastructure: the human factor. DOI:10.1007/s11227-018-2337-2

27. Krombholtz, K. et al. (2013). Social Engineering Attacks on the Knowledge Worker. Proceedings of the 6th International Conference on Security of Information and Networks. Retrieved from: https://publications.sba-research.org/publications/sig-alternate.pdf

28. Kronberg, B., Swanlund, J., Jeppsson, H. (2015). Social Engineering. A study in awareness and measures. Retrieved from: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=5474076&fileOId=5474079