https://doi.org/10.31649/2524-1079-2024-9-1-037-042

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ: МЕТОДИ ЗАПОБІГАННЯ ТА ЗАХИСТУ

Олексій Жмурко[1], orcid.org/0009-0004-0226-8470, e-mail: oleksijzmurko47@gmail.com

1. Вінницький національний технічний університет, Вінниця

Актуальність дослідження соціальної інженерії обумовлена постійно зростаючою кількістю кібератак, що використовують людський фактор як основний вектор проникнення. Зловмисники, застосовуючи різноманітні методи, такі як фішинг, вішинг, претекстинг та інші, завдають значних збитків організаціям, викрадаючи конфіденційні дані, підриваючи репутацію та порушуючи безперебійну роботу бізнес-процесів. Зростання кібератак, пов’язаних із соціальною інженерією, вимагає вдосконалення законодавчої бази та розробки нових стандартів кібербезпеки.

У статті проаналізовано сучасні методи соціальної інженерії, їхній вплив на інформаційні системи та організації, а також визначено основні напрямки захисту від цих загроз. Особлива увага приділена ролі людського фактору в кібербезпеці та необхідності комплексного підходу, що поєднує в собі технічні, організаційні та освітні заходи. Окрему увагу приділено викликам, пов'язаним із людським фактором у системах кібербезпеки, а також важливості комплексного підходу до боротьби з цими загрозами. Обґрунтовано необхідність інтеграції програм навчання та тренувань із кібербезпеки для зменшення ризику успішних атак соціальної інженерії.

Визначено перспективи подальших досліджень, зокрема в напрямку розробки інтерактивних навчальних програм для підвищення обізнаності користувачів та розробці нових алгоритмів для автоматичного виявлення спроб соціальних атак.

Ключові слова: соціальна інженерія, кібербезпека, методи запобігання, захист, інформаційна безпека, вдосконалення професійної підготовки, фахівців в галузі цифрових технологій.

Постановка проблеми. У сучасному цифровому світі соціальна інженерія є однією з найбільших загроз для кібербезпеки. Цей метод базується на маніпуляції людьми з метою отримання конфіденційної інформації або доступу до систем, обходячи технологічні засоби захисту. Соціальна інженерія охоплює різноманітні прийоми, такі як фішинг, вішинг, бейтинг та інші, що використовують психологічний вплив на жертв. Зважаючи на людський фактор, соціальна інженерія є особливо небезпечною, адже її складно виявити та запобігти лише за допомогою технічних засобів. Атаки цього типу можуть мати серйозні наслідки для організацій та індивідуальних користувачів, включаючи втрату даних, фінансові втрати та репутаційні ризики. Тому проблема захисту від соціальної інженерії стає все більш актуальною.

Потреба в розробці ефективних методів запобігання таким атакам є критично важливою для забезпечення кібербезпеки. Надзвичайно важливо навчати студентів методам протидії соціальній інженерії, адже майбутні фахівці в галузі цифрових технологій будуть працювати з великими обсягами даних і матимуть доступ до важливої інформації. Включення таких курсів у освітні програми сприятиме формуванню навичок розпізнавання та запобігання атакам. Відтак, важливо розуміти, що соціальна інженерія постійно еволюціонує. Зловмисники розробляють все більш складні методи маніпуляції. Тому, окрім навчання теоретичним основам, потрібно проводити практичні заняття, симуляції атак, щоб студенти мали можливіть набувати досвіду з розпізнавання різних видів шахрайства. Впровадження таких програм навчання дозволить підготувати фахівців, які зможуть ефективно протидіяти сучасним кіберзагрозам і убезпечити роботу інформаційних систем.

Аналіз наукових досліджень і публікацій. Проблематика соціальної інженерії є предметом дослідження багатьох науковців. Так, В. Нам’ясенко (2019) вважає, що соціальна інженерія є сукупністю знань, які дозволяють систематично створювати, змінювати та підтримувати нові соціальні системи, а Н. Драгомирецька (2015), що вона спрямована на формування стійких моделей розвитку територій через оптимізацію взаємодії між суб’єктами державного управління та громадськістю, з метою подолання соціальної поляризації. Автор J.-W.Bullee (2017) трактує соціальну інженерію як метод кібератак, який використовує знання з соціальних наук для маніпулювання людьми з метою

отримання доступу до інформації або систем. Шляхом створення штучних соціальних ситуацій та використання вразливостей людської психології зловмисник досягає бажаного результату. У статті А. Мельниченко (2012) проведено аналіз ролі соціальної інженерії у контексті сталого розвитку. Автор досліджує різноманітні теоретичні підходи до цього поняття, обґрунтовуючи його потенціал для вирішення сучасних соціальних проблем та побудови більш справедливого суспільства.

Дослідниця О. Козицька (2021) зосередила увагу на застосуванні принципів соціальної інженерії як методологічного інструменту в криміналістичному дослідженні. На думку науковиці, соціальна інженерія, яка базується на психологічному впливі, є ефективним методом кіберрозвідки і може бути використана слідчими та оперативними працівниками для виявлення, розкриття та розслідування кримінальних правопорушень. Вона пропонує розглядати соціальну інженерію як інструмент для виконання тактичних завдань, таких як ідентифікація осіб за цифровими слідами, отримання криміналістично значущої інформації та спонукання осіб до певних дій або утримання від них.

У статті Л. Половенко та С. Мерінової (2019) проведено комплексне дослідження феномену соціальної інженерії в контексті економічної безпеки підприємства. За допомогою інструментарію економіко-математичного моделювання та інтелектуального аналізу автори виявили основні методи та шляхи атак соціальних хакерів, зосередившись на використанні таких людських факторів, як довіра та цікавість. На підставі отриманих результатів розроблено рекомендації щодо підвищення стійкості підприємств до соціальних атак. В. Соколов і Д. Курбанмурадов (2018) розробляють комплексні заходи та стратегії, спрямовані на захист інформаційних систем та даних від загроз, пов’язаних з маніпулятивними діями зловмисників.

Цікавим в контексті нашого дослідження є публікація Т. Ткач (2013), у якій аналізуються соціотехнічні аспекти проектування систем людської діяльності з акцентом на їхній вплив на освітній процес. Розглядаються механізми інтеграції соціальних і психологічних факторів у процесі конструювання освітніх середовищ. Автор дослідження розширює межі проектування, включаючи в нього не тільки матеріальні об'єкти, але й особистісний розвиток здобувача, зміст освіти та виховання.

Окремі аспекти забезпечення безпеки в контексті соціальної інженерії розглянуті в публікаціях М. Шатковського (2015), М. Ганченко (2022), Ю. Якименка, Д. Рабчуна, М. Запорожченка (2021), S. Zhurin, D. Komarkov (2018), D. Jampen, G. Gür, T. Sutter, B. Tellenbach (2020) та інших.

Мета статті – здійснити комплексне дослідження сучасних методів соціальної інженерії, проаналізувати їхній вплив на кібербезпеку та розробити рекомендації щодо підвищення обізнаності здобувачів із ефективними заходами захисту.

Виклад основного матеріалу. Соціальна інженерія – це стратегія комунікації, яка використовує психологічні прийоми для досягнення бажаного впливу на аудиторію. Її суть полягає в створенні та трансляції повідомлень, що резонують з існуючими потребами та страхами цільової аудиторії, з метою спонукання її до певних дій. Розвиток цифрових комунікаційних каналів суттєво розширив можливості застосування соціальної інженерії, перетворивши її на ефективний інструмент як для реклами, так і для інших видів впливу. Шляхом виявлення та експлуатації вразливостей людської психології, таких як довіра, бажання належати до певної соціальної групи або страху втрати формують у користувача бажаний образ ситуації або пропонують вирішення проблем, спонукаючи до певних дій. Сучасні комунікаційні технології, зокрема соціальні мережі, електронна пошта та месенджери, значно розширили арсенал інструментів соціальних інженерів, дозволяючи їм досягати широкої аудиторії та персоналізувати свої повідомлення. Завдяки цьому, соціальна інженерія стала потужним інструментом у сферах маркетингу, політики та кібербезпеки. Ключові елементи соціальної інженерії наведені на рисунку 1.

Прикладами психологічних маніпуляцій, що використовуються в рамках соціальної інженерії для отримання конфіденційної інформації або доступу до систем, є такі:

1. Фішинг (phishing), зміст якого полянає в тому, що зловмисники надсилають електронні листи або повідомлення, що виглядають як офіційні, наприклад, від банку або компанії. У них містяться посилання на фальшиві веб-сайти, де жертва вводить свої паролі, номери кредитних карток або іншу конфіденційну інформацію.

2. Смішинг (smishing) – варіант фішингу через SMS. Зокрема, жертва отримує повідомлення з проханням перейти за посиланням або зателефонувати на номер для підтвердження даних, що призводить до втрат її приватної інформації або грошей.

3. Вішинг (vishing) – це телефонні шахрайства, коли зловмисники видають себе за представників компанії або служби підтримки. Вони можуть просити надати конфіденційну інформацію або змусити жертву виконати дії, що відкриють доступ до системи.

4. Клонування сайтів (website spoofing). Зловмисник створює копію реального сайту (зокрема, веб-сайт банку) та спонукає жертву відвідати його та ввести свої дані.

5. Захоплення профілю (impersonation). Зловмисник видає себе за довірену особу в онлайн-спілкуванні або соціальних мережах, щоб обманом отримати від жертви інформацію або змусити її виконати певні дії.

6. Атаки через соціальні мережі, коли шахраї використовують соціальні мережі для збору інформації про цільову жертву або надсилають фальшиві запити про дружбу від імені знайомих для отримання доступу до особистих даних.

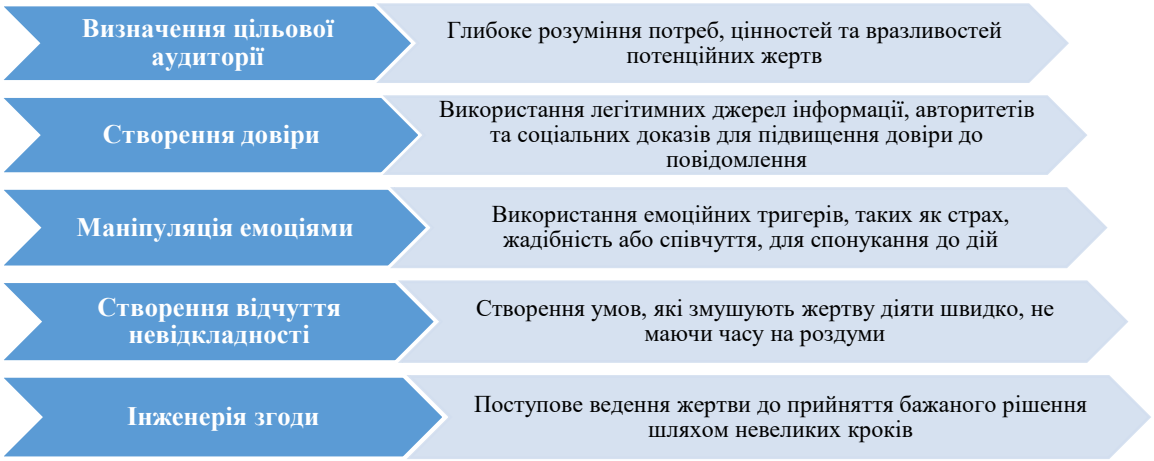

Рисунок 1 – Ключові елементи соціальної інженерії

Соціальна інженерія є потужним інструментом, який може бути використаний як для досягнення позитивних цілей, таких як підвищення обізнаності про соціальні проблеми чи мобілізація громадськості, так і для здійснення злочинних дій. Розуміння принципів соціальної інженерії є важливим для захисту себе та своїх даних від кіберзагроз, а також для розробки ефективних стратегій протидії дезінформації та маніпуляції свідомістю. Вважаємо доцільним звернути увагу здобувачів на такі аспекти:

1. Потреба в постійному навчанні та підвищенні обізнаності про кібербезпеку. Соціальна інженерія, що традиційно використовується зловмисниками для отримання доступу до конфіденційної інформації, може бути ефективно застосована в освітніх цілях. Імітовані кібератаки, такі як фішинг, вішинг, або створення фальшивих веб-сайтів, дозволяють створити реалістичне середовище для навчання співробітників і користувачів. Шляхом участі в таких симуляціях люди набувають практичного досвіду в розпізнаванні та відхиленні потенційних загроз.

2. Навчання ефективним методам оцінювання стійкості інформаційних систем. У процесі оцінювання стійкості інформаційних систем широкого застосування набув метод пентестингу. Одним із ключових компонентів такого тестування є використання методів соціальної інженерії. Застосування психологічних маніпуляцій дозволяє виявити не лише технічні вразливості системи, а й слабкі місця в поведінці персоналу. Це дозволяє ідентифікувати потенційні вектори атак, пов’язані з людським фактором, та вжити заходів для їх усунення до того, як ними скористаються зловмисники. Зокрема, на основі результатів пентестингу можуть бути оновлені правила доступу до інформаційних ресурсів, посилені алгоритми шифрування даних, а також розроблені нові процедури навчання персоналу з метою формування безпечної поведінки.

3. Використання соціальної інженерії для покращення політики безпеки компанії. Результати тестів соціальної інженерії можуть сприяти розробленню та впровадженню ефективніших політик безпеки. Зокрема, після імітованих атак організації часто оновлюють правила доступу, шифрування даних, або навіть поведінкові протоколи співробітників.

4. Формування культури інформаційної безпеки через систематичне навчання та оцінювання вразливостей, пов’язаних з людським фактором. Регулярне проведення навчальних заходів і симуляцій кібератак з використанням методів соціальної інженерії сприяє формуванню стійкої культури інформаційної безпеки в організації. Систематична оцінка вразливостей, пов’язаних з людським

фактором, дозволяє підвищити рівень обізнаності співробітників щодо потенційних загроз, розвинути критичне мислення та відповідальне ставлення до питань безпеки інформації. Як результат, зменшується ймовірність успішних кібератак, пов'язаних з помилками персоналу.

5. Вдосконалення навичок комунікації та співпраці. Залученість співробітників різних підрозділів організації до сценаріїв симульованих кібератак, що базуються на методах соціальної інженерії, сприяє не лише підвищенню рівня обізнаності щодо потенційних загроз, а й стимулює ефективну міжвідомчу взаємодію. Спільна робота над розробкою та впровадженням заходів реагування на виявлені небезпеки сприяє формуванню єдиної культури інформаційної безпеки в організації та підвищує її стійкість до кіберзагроз.

6. Застосування методів соціальної інженерії в благодійній діяльності. Деякі благодійні організації використовують принципи соціальної інженерії для розробки ефективних комунікаційних заходів, спрямованих на залучення громадськості до участі в благодійних проектах. За допомогою психологічних механізмів, що лежать в основі соціальної інженерії, організації прагнуть мотивувати людей до здійснення благодійних внесків та активної участі в соціальних ініціативах.

7. Ідентифікація та профілактика внутрішніх загроз за допомогою методів соціальної інженерії. Методи соціальної інженерії можуть бути використані для ефективного виявлення потенційних внутрішніх загроз, таких як шахрайські дії з боку персоналу або несанкціоноване використання корпоративних ресурсів. Шляхом моделювання реальних сценаріїв соціальної інженерії можна ідентифікувати слабкі місця в поведінці співробітників і розробити проактивні заходи для запобігання інцидентам, які пов'язані з людським фактором.

Висновки та перспективи подальших наукових досліджень. Отже, соціальна інженерія, як метод маніпулятивного впливу на користувачів з метою отримання конфіденційної інформації, становить серйозну загрозу сучасній кібербезпеці. На відміну від технічних атак, які базуються на експлуатації вразливостей програмного забезпечення, соціальна інженерія експлуатує людський фактор, зокрема довіру та допитливість користувачів. Типові методи соціальної інженерії включають фішинг, вішинг, претекстинг та інші, які передбачають використання різноманітних психологічних маніпуляцій для примушення жертви розкрити конфіденційні дані або виконати шкідливі дії. Наслідки успішних атак соціальної інженерії можуть бути катастрофічними, включаючи фінансові втрати, репутаційні ризики та порушення безперебійної роботи організацій.

Для ефективного протистояння соціальній інженерії потрібно застосування комплексного підходу, що поєднує технічні та організаційні заходи безпеки. З одного боку, важливо впроваджувати сучасні технології захисту інформації, такі як системи виявлення вторгнень, фільтри спаму та багатофакторну аутентифікацію. З іншого боку, потрібно проводити регулярні навчання персоналу з метою підвищення обізнаності про методи соціальної інженерії та формування навичок розпізнавання підозрілих дій. Ключовим аспектом захисту від небезпек із застосуванням соціальної інженерії є створення культури безпеки в організації. Кожен співробітник повинен володіти навичками розпізнавання та оцінки соціального інжинірингу. Систематичне оновлення знань про сучасні методи маніпуляції є ключовим фактором у протидії таким загрозам. Незалежно від рівня займаної посади, всі працівники повинні бути поінформовані про потенційні ризики та способи їхньої нейтралізації.

Подальші наукові дослідження будуть спрямовані на розробку більш ефективних методів виявлення та протидії загрозам соціальній інженерії, а також на аналіз еволюції тактик зловмисників у контексті нових технологій. Особливу увагу потрібно приділити дослідженню психологічних аспектів соціальної інженерії, розробці інтерактивних навчальних програм для підвищення обізнаності користувачів і розробці нових алгоритмів для автоматичного виявлення спроб соціальних атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

Bullee, J.-W. (2017). *Experimental Social Engineering: Investigation and Prevention* (dissirtation to obtain the degree or doctor at the University of Twente). Enschede, The Niderland. doi: 10.3990/1.9789036543972.

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences,* 10(1). https://doi.org/10.1186/s13673-020-00237-7

Zhurin, S. I., & Komarkov, D. E. (2018). Protection of external information perimeter of organization from spear phishing. *Bezopasnost informacionnyh tehnology,* 25(4), 96–108. https://doi.org/10.26583/bit.2018.4.09

Ганченко, М. І. (2022). Людський психологічний та біометричний фактор у розвитку та використанні

методів соціальної інженерії у мирний та воєнний час. *Сучасний захист інформації*, 1 (49), 16-26. DOI: 10.31673/2409-7292.2022.011626

Драгомирецька, Н. М. (2015). Сучасне зарубіжне розуміння соціальної інженерії та її можливості в державному управлінні. *Теорія та практика державного управління і місцевого самоврядування,* 2. URL: http://el-zbirndu.at.ua/2015_2/32.pdf

Козицька, О. Г. (2021). Використання методу соціальної інженерії в процесі виявлення, розкриття та розслідування кримінальних правопорушень. *Юридична психологія*, 1 (28), 34-40.

Мельниченко, А. А. (2012). Соціальна інженерія як фактор забезпечення стійкого розвитку соціальних систем. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право,* 1 (13). https://visnyk-psp.kpi.ua/article/view/123398.

Нам'ясенко, В.М. (2016). Соціальна інженерія як одна із загроз економічній безпеці, що спричиняє негативний вплив на ефективність діяльності підприємства. *Економіка та держава*, 3, 90–92

Половенко, Л., & Мерінова, С. (2019). Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві. *Підприємництво та інновації*, (10), 183-187. https://doi.org/10.37320/2415-3583/10.28

Соколов, В. Ю., & Курбанмурадов, Д. М. (2018). Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. *Кібербезпека: освіта, наука, техніка*, 1 (1), 6-16.

Ткач, Т. В. (2013). Системний аналіз та соціальна інженерія як методи проектування освітнього простору. *Збірник наукових праць Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна «Проблеми економіки транспорту»,* 5, 30-36.

Шатковський, М. О. (2015). Вплив соціальної інженерії на інформаційну безпеку організацій. Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», м. Київ, 21-23 травня 2015. Київ : НТУУ «КПІ», 216-219.

Якименко, Ю. М., Рабчун, Д. І., & Запорожченко, М. М. (2021). Місце соціальної інженерії в проблемі витоку даних та організаційні аспекти захисту корпоративного середовища від фішингових атак з використанням електронної пошти. *Кібербезпека: освіта, наука, техніка*, 1 (13). DOI 10.28925/2663-4023.2021.13.615

REFERENCES

Bullee, J.-W. (2017). *Experimental Social Engineering: Investigation and Prevention* (dissirtation to obtain the degree or doctor at the University of Twente). Enschede, The Niderland. doi: 10.3990/1.9789036543972. [in English].

Drahomyretska, N. M. (2015). Suchasne zarubizhne rozuminnia sotsialnoi inzhenerii ta yii mozhlyvosti v derzhavnomu upravlinni [Modern foreign understanding of social engineering and its possibilities in public administration]. *Teoriia ta praktyka derzhavnoho upravlinnia i mistsevoho samovriaduvannia,* 2. URL: http://el-zbirndu.at.ua/2015_2/32.pdf. [in Ukrainian].

Hanchenko, M. I. (2022). Liudskyi psykholohichnyi ta biometrychnyi faktor u rozvytku ta vykorystanni metodiv sotsialnoi inzhenerii u myrnyi ta voiennyi chas [Human psychological and biometric factors in the development and use of social engineering methods in peacetime and wartime]. *Suchasnyi zakhyst informatsii,* 1 (49), 16-26. DOI: 10.31673/2409-7292.2022.011626. [in Ukrainian].

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences,* 10(1). https://doi.org/10.1186/s13673-020-00237-7. [in English].

Kozytska, O. H. (2021). Vykorystannia metodu sotsialnoi inzhenerii v protsesi vyiavlennia, rozkryttia ta rozsliduvannia kryminalnykh pravoporushen [Use of the social engineering method in the process of detection, disclosure and investigation of criminal offenses]. *Yurydychna psykholohiia*, 1 (28), 34-40. [in Ukrainian].

Melnychenko, A. A. (2012). Sotsialna inzheneriia yak faktor zabezpechennia stiikoho rozvytku sotsialnykh system [Social engineering as a factor in ensuring the sustainable development of social systems]. *Visnyk NTUU «KPI». Politolohiia. Sotsiolohiia. Pravo,* 1 (13). https://visnyk-psp.kpi.ua/article/view/123398. [in Ukrainian].

Namiasenko, V.M. (2016). Sotsialna inzheneriia yak odna iz zahroz ekonomichnii bezpetsi, shcho sprychyniaie nehatyvnyi vplyv na efektyvnist diialnosti pidpryiemstva [Social engineering as one of the threats to economic security, which causes a negative impact on the efficiency of the enterprise]. *Ekonomika ta derzhava*, 3, 90–92. [in Ukrainian].

Polovenko, L., & Merinova, S. (2019). Vyiavlennia oznak sotsialnoi inzhenerii ta tekhnolohiia protydii sotsialnym khakeram na pidpryiemstvi [Identification of signs of social engineering and technology to counter social hackers in the enterprise]. *Pidpryiemnytstvo ta innovatsii*, (10), 183-187. https://doi.org/10.37320/2415-3583/10.28. [in Ukrainian].

Shatkovskyi, M. O. (2015). Vplyv sotsialnoi inzhenerii na informatsiinu bezpeku orhanizatsii [The influence of social engineering on the information security of organizations]. Materialy XIII Vseukrainskoi naukovo-praktychnoi konferentsii studentiv, aspirantiv ta molodykh vchenykh «Teoretychni i prykladni problemy fizyky, matematyky ta informatyky», m. Kyiv, 21-23 travnia 2015. Kyiv : NTUU «KPI», 216-219. [in Ukrainian].

Sokolov, V. Yu., & Kurbanmuradov, D. M. (2018). Metodyka protydii sotsialnomu inzhynirynhu na obiektakh informatsiinoi diialnosti [Methods of countering social engineering at the objects of information activity]. *Kiberbezpeka: osvita, nauka, tekhnika*, 1(1), 6–16. [in Ukrainian].

Tkach, T. V. (2013). Systemnyi analiz ta sotsialna inzheneriia yak metody proektuvannia osvitnoho prostoru [System analysis and social engineering as methods of designing educational space]. *Zbirnyk naukovykh prats Dnipropetrovskoho natsionalnoho universytetu zaliznychnoho transportu imeni akademika V. Lazariana «Problemy ekonomiky transportu»*, 5, 30-36. [in Ukrainian].

Yakymenko, Yu. M., Rabchun, D. I., & Zaporozhchenko, M. M. (2021). Mistse sotsialnoi inzhenerii v problemi vytoku danykh ta orhanizatsiini aspekty zakhystu korporatyvnoho seredovyshcha vid fishynhovykh atak z vykorystanniam elektronnoi poshty [The place of social engineering in the problem of data leakage and organizational aspects of protecting the corporate environment from phishing attacks using e-mail]. *Kiberbezpeka: osvita, nauka, tekhnika*, 1 (13). DOI 10.28925/2663-4023.2021.13.615. [in Ukrainian].

Zhurin, S. I., & Komarkov, D. E. (2018). Protection of external information perimeter of organization from spear phishing. *Bezopasnost informacionnyh tehnology*, 25(4), 96–108. https://doi.org/10.26583/bit.2018.4.09. [in English].

Олексій Жмурко – аспірант кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, Вінниця, e-mail: oleksijzmurko47@gmail.com.

SOCIAL ENGINEERING AS A THREAT TO CYBERSECURITY: METHODS OF PREVENTION AND PROTECTION

Oleksii Zhmurko – Postgraduate Student, Department of Life Safety and Safety Pedagogy, Vinnytsia National Technical University, Vinnytsia, e-mail: oleksijzmurko47@gmail.com.

The relevance of the study of social engineering is due to the ever-growing number of cyberattacks that use the human factor as the main penetration vector. Attackers, using various methods such as phishing, vishing, pretexting, and others, cause significant damage to organisations by stealing confidential data, undermining reputation, and disrupting the smooth operation of business processes. The growth of social engineering-related cyberattacks requires improving the legal framework and developing new cybersecurity standards.

The article analyses modern methods of social engineering, their impact on information systems and organisations, and identifies the main areas of protection against these threats. Particular attention is paid to the role of the human factor in cybersecurity and the need for an integrated approach that combines technical, organisational and educational measures. Particular attention is paid to the challenges associated with the human factor in cybersecurity systems, as well as the importance of an integrated approach to combating these threats. The author substantiates the need to integrate cybersecurity education and training programmes to reduce the risk of successful social engineering attacks.

Prospects for further research are identified, in particular in the development of interactive training programmes to raise user awareness and the development of new algorithms for the automatic detection of social attack attempts

Keywords: social engineering, cybersecurity, prevention methods, protection, information security, improvement of professional training, digital specialists.

Дата надходження статті до редакції: 21 березня 2024 р.