УДК 004.056.5

В. Ю. Постемська
Т. Г. Кирилащук

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ОСНОВНА ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Вінницький національний технічний університет

Анотація

У тезі розглянуто поняття «соціальна інженерія» та проаналізовано її як одну з провідних загроз інформаційній безпеці. Охарактеризовано основні методи соціальної інженерії, зокрема фішинг, вішинг, претекстинг, бейтинг та смішинг. Визначено причини ефективності таких атак, пов'язані з людським фактором, довірою та недостатнім рівнем обізнаності користувачів. Окреслено практичні заходи протидії соціальній інжерерії в організаціях та приватному секторі.

Ключові слова: соціальна інженерія, інформаційна безпека, фішинг, кіберзагрози, людський фактор.

Abstract

The thesis examines the concept of social engineering and analyzes it as one of the main threats *to information security. The main methods of social engineering are characterized, including phishing, vishing, pretexting, baiting and smishing. The reason for the effectiveness of such attacks related to the human factor, trust and insufficient user awareness are identified. Practical measures for preventing social engineering attacks in organizations and the private sector are outlined.*

Keywords: social engineering, information security, phishing, cyber threats, human factor.

Вступ

Інформаційні системи організацій захищені технічними засобами: міжмережевими екранами, антивірусним програмним забезпеченням, системами виявлення вторгнень. Проте значна частина інцидентів виникає через маніпуляції людьми, які мають доступ до даних. Соціальна інженерія спрямована саме на використання психологічних особливостей людини для отримання конфіденційної інформації або несанкціонованого доступу до ресурсів. Зростання кількості дистанційної роботи, онлайн-сервісів та електронного документообігу розширює поле для атак. Зловмисники дедалі частіше комбінують технічні засоби з психологічним впливом, що підвищує результативність їхніх дій.

Результати дослідження

Соціальна інженерія – це сукупність методів психологічного впливу, спрямованих на спонукання людини до розкриття конфіденційної інформації або виконання дій, які суперечать правилам безпеки. На відміну від технічного зламу у центрі атаки перебуває людини. [1]

Найпоширеніші методами соціальної інженерії:

1. Фішинг – розсилання електронних повідомлень або створення підроблених веб-сайтів з метою отримання логінів, паролів, банківських реквізитів.
2. Вішинг – телефонні дзвінки, під час яких зловмисник представляється працівником банку чи іншої установи та намагається отримати персональні дані.
3. Претекстинг – створення вигаданої ситуації або ролі для отримання довіри жертви.
4. Бейтинг – використання шахраями привабливих пропозицій, тобто безкоштовного контенту, послуг чи подарунків.

5. Смішинг – вид шахрайства, коли зловмисник використовує фішингові SMS, щоб заволодіти конфіденційною інформацією.[2]

Ефективність соціальної інженерії зумовлена поєднанням організаційних недоліків і психологічних особливостей поведінки користувачів. Низький рівень цифрової грамотності ускладнює розпізнавання фішингових повідомлень, підроблених веб-ресурсів або маніпулятивних телефонних дзвінків. Відсутність систематичного навчання з питань кібербезпеки призводить до того, що люди не оновлюють знання про нові схеми шахрайства та діють за застарілими уявленнями про загрози. Довіра до повідомлень, які зовні виглядають як офіційні, без додаткової верифікації створює сприятливі умови для зловмисників. Додатковим фактором ризику є відсутність чітко визначених процедур реагування на підозрілі звернення, через що працівники не знають, як діяти в потенційно небезпечній ситуації. У результаті саме людський фактор стає точкою входу для компрометації навіть технічно захищених інформаційних систем.

Суттєву роль відіграють і психологічні механізми, на яких базуються атаки соціальної інженерії. Зловмисники використовують авторитет, терміновість або страх втрати доступу до сервісів, щоб спонукати користувача швидко прийняти рішення без перевірки інформації. Поширеною є практика маскування під представників технічної підтримки, керівництва компанії або фінансових установ. У таких випадках люди схильні виконувати отримані інструкції через звичку довіряти офіційним структурам. Додатково використовуються методи психологічного тиску, коли користувача переконують діяти негайно, щоб уникнути блокування облікового запису або фінансових втрат.[3]

Ризики посилюються через активне використання електронної пошти, соціальних мереж і корпоративних месенджерів. Через ці канали зловмисники збирають відкриту інформацію про співробітників, структуру організації та внутрішні процеси. Отримані відомості дозволяють формувати цільові атаки, у яких повідомлення виглядають максимально переконливо. Такий підхід підвищує ймовірність того, що користувач відкриє шкідливе вкладення, перейде за фішинговим посиланням або передасть конфіденційні дані.

Протидія соціальній інженерії потребує системного підходу, що поєднує організаційні та технічні заходи. Регулярні тренінги з моделюванням реальних сценаріїв атак підвищують здатність розпізнавати маніпулятивні дії та формують навички безпечної поведінки під час роботи з інформаційними системами. Доцільним є впровадження багатофакторної автентифікації, яка зменшує ризик несанкціонованого доступу навіть у разі компрометації облікових даних. Обмеження доступу до критичних ресурсів і застосування принципу мінімальних привілеїв зменшують масштаб можливих наслідків інциденту. [4]

Постійний моніторинг підозрілої активності дозволяє швидко виявляти не типові дії користувачів або спроби вторгнення. Для цього використовують системи аналізу журналів подій, засоби виявлення вторгнень та інструменти поведінкової аналітики. Важливим елементом є розроблення чітких інструкцій щодо перевірки фінансових операцій та запитів на передачу конфіденційної інформації.

Окрему увагу приділяють формуванню культури інформаційної безпеки. Люди повинні розуміти потенційні наслідки витоку даних або несанкціонованого доступу. За наявності зрозумілих процедур, повідомлення про підозрілі події частіше інформують службу безпеки про підозрілі листи, дзвінки або повідомлення. Такий підхід дозволяє виявляти атаки на ранніх етапах і зменшує ймовірність успішної реалізації шахрайських схем.

Висновок

Отже, соціальна інженерія становить суттєву загрозу інформаційній безпеці, оскільки спрямована на використання поведінкових та психологічних особливостей людини. На відміну від суто технічних атак, вона дозволяє зловмисникам отримувати доступ до конфіденційних даних через

маніпуляцію довірою, неуважністю або недостатньою обізнаністю користувачів. Аналіз основних методів соціальної інженерії та чинників їх ефективності свідчить, що ключовим елементом захисту є не лише технічна інфраструктура, а й підготовлений персонал. Підвищення рівня цифрової грамотності, впровадження чітких процедур реагування та системне навчання працівників формують стійкість організацій до таких атак і зменшують ризик компрометації інформаційних ресурсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is Social Engineering? - Meaning. /. URL: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering (date of access: 24.02.2026).

2. Державна служба спеціального зв'язку та захисту інформації України. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/faqs/60-kiberatak-pochinayetsya-z-fishingu-chas-pidvishiti-pilnist (дата звернення: 24.02.2026).

3. Соціальна інженерія – що це таке, атаки з використанням соціальної інженерії. ESET. *ESET*. URL: https://www.eset.com/ua/support/information/entsyklopediya-zahroz/sotsialna-inzheneriya/?srsltid=AfmBOorsf4bdkzQZT7DoylWwawzkm0SzTULhS9pa0hG8Jhea0GiTD6yJ (дата звернення: 13.03.2026).

4. Федоришин О. О. Методи протидії соціальній інженерії для пересічного користувача інтернету / О. О. Федоришин // Кваліфікаційні бакалаврські роботи. Донецький національний університет імені Василя Стуса. – 2024. – № 1. – ст. 36

Вероніка Юріївна Постемська – студентка групи 2КІТС-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, email: veronikapostemska@gmail.com.

Науковий керівник: **Кирилащук Тетяна Григорівна** – асистент кафедри інформації захисту, Вінницький національний технічний університет, Вінниця. kgt0998@gmail.com

Veronika Y. Postemska – student of group 2KITS-24b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: veronikapostemska@gmail.com.

Scientific Supervisor: **Tetiana H. Kyrylashchuk** – assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia. kgt0998@gmail.com