УДК

Глущенко А. В.

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ВИД КІБЕРШАХРАЙСТВА

Вінницький національний технічний університет

Анотація

Більшість методів соціальної інженерії не вимагають особливих технічних знань з боку зловмисників, а отже використовувати ці методи може будь-хто — від дрібних злодіїв до досвідчених кіберзлочинців.

Ключові слова: соціальна інженерія; зловмисники; методи; кіберзлочинці.

Abstract

Most social engineering methods do not require any special technical knowledge on the part of attackers, which means that anyone can use them — from petty thieves to experienced cybercriminals.

Keywords: social engineering; attackers; methods; cybercriminals.

Вступ

Хоча кібербезпека традиційно зосереджується на технічних засобах захисту, такі як брандмауер, антивірус і шифрування, найвразливішою ланкою все ж залишається людина. Соціальна інженерія використовує психологічні чинники, такі як довіра, страх, терміновість або авторитет, щоб змусити користувачів добровільно розкрити конфіденційні дані чи надати доступ до систем. Саме тому більшість сучасних кібератак починається не зі зламу програмного коду, а з маніпуляції поведінкою користувача.

Результати дослідження

Соціальна інженерія – це вид шахрайства, основна мета якого отримати доступ до конфіденційної інформації завдяки психологічному впливу на людину [1]. Соціальна інженерія з точки зору кібербезпеки розглядається як одна з найнебезпечніших і водночас найефективніших форм атак, оскільки вона спрямована не на технічні вразливості систем, а на людський фактор. У сучасних дослідженнях підкреслюється, що навіть найкраще налаштований брандмауер або система шифрування може бути обійдена, якщо зловмисник переконає співробітника добровільно надати доступ або розкрити конфіденційну інформацію.

Глобальне дослідження Scamadviser, в якому брали участь 48 країн, свідчить, що 76% людей упевнені, що зможуть ідентифікувати аферистів, однак 73% з них, зіткнувшись із шахрайством, все одно розголошують усі конфіденційні дані, необхідні зловмисникам [2].

Майбутня боротьба із соціальною інженерією, ймовірно, буде передбачати поєднання вдосконалених технологічних рішень та підвищеної людської обізнаності [3]. З поширенням безпарольної аутентифікації вона відіграватиме ключову роль у зменшенні багатьох традиційних ризиків соціальної інженерії.

У кіберконтексті соціальна інженерія проявляється як основний інструмент кіберзлочинців для отримання доступу до приватних даних, рахунків, систем корпоративної безпеки або навіть інфраструктур критичних систем [4]. Сучасні дослідження з кібербезпеки демонструють, що успішні атаки починаються не з технічного злому сервера чи виявлення уразливого коду, а з маніпулювання поведінкою людей – співробітників, користувачів, адміністраторів.

Соціальні інженери застосовують різні техніки, але найпоширенішими в контексті кібербезпеки є:

1. Фішинг – розповсюдження листів, що маскуються під легітимні повідомлення від банків, сервісів чи колег, з метою змусити користувача ввести пароль або перейти на шкідливий сайт. Це одна з найчастіших форм атак, оскільки листи можуть бути масштабовані й автоматизовані.

2. Соціальна маніпуляція через телефонні дзвінки (vishing) – зловмисники телефонують співробітникам, видають себе за IT-службу або техпідтримку, і під приводом «вирішення проблеми» змушують надати доступ або дані. Такий тип атаки був використаний у реальному випадку з великою авіакомпанією, де телефонний дзвінок став початковою точкою витоку персональних даних мільйонів клієнтів.

3. AI-підсилені атаки – сучасні дослідження показують, що генеративний штучний інтелект значно підвищує якість соціальних інженерних атак, дозволяючи створювати реалістичний персоналізований контент (листи, повідомлення, голосові записи), який важче відрізнити від справжнього. Це означає, що атакувальники можуть ускладнювати захист і робити фейкові повідомлення чи аудіо значно переконливішими.

4. Ці методи не вимагають глибоких технічних знань, достатньо лише знання базових психологічних механізмів: як змусити людину довіряти, відчувати терміновість чи страх, реагувати на імперський авторитет або «вигоду» [5]. Саме ці психологічні мотиви роблять соціальну інженерію ефективною, навіть проти технічно захищених систем.

5. Одне з ключових наукових досліджень у цій сфері – аналіз участі людей у фішингових кампаніях на реальних робочих місцях показує, що до 82% витоків інформації включають людський фактор, де співробітники або натискають на шкідливі посилання, або не повідомляють про підозрілі листи [6]. Це підкреслює, що вразливість не лише технічна, але й поведінкова, і залежить від демографії, рівня підготовки та культури кібербезпеки в організації.

Висновки

Отже, можна зробити висновок, що ефективність кібербезпеки залежить не лише від рівня технічного захисту, а й від підготовленості та обізнаності користувачів. Оскільки соціальна інженерія спрямована насамперед на людський фактор, саме люди стають головною мішенню зловмисників. Тому поряд із впровадженням сучасних технологічних рішень необхідно приділяти особливу увагу розвитку критичного мислення, цифрової грамотності та культури безпечної поведінки в інформаційному середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Соціальна інженерія: що це та як уберегтися від шахрайства. *ZEN.COM*. URL: https://www.zen.com/ua/blog/personal-finance-uk/social-engineering-how-to-protect-yourself-from-fraud/ (дата звернення: 19.02.2026).
2. Соціальна інженерія – головний інструмент шахрая. *Гаразд*. URL: https://harazd.bank.gov.ua/article/sahrajstvo/platizne-sahrajstvo/socialna-inzeneria-golovnij-instrument-sahraa (дата звернення: 19.02.2026).
3. Що таке соціальна інженерія в кібербезпеці? [Приклади та поради] | Hideez. *Passwordless Workforce Identity Solutions | Hideez*. URL: https://hideez.com/uk-ua/blogs/news/social-engineering (дата звернення: 19.02.2026).
4. Соціальна інженерія як загроза кібербезпеці: методи запобігання та захисту | Педагогіка безпеки. Педагогіка безпеки. URL: https://pedbezpeka.vntu.edu.ua/index.php/pb/article/view/151 (дата звернення: 19.02.2026).
5. Social Engineering Attacks in Cybersecurity. International Journal & Research Paper Publisher | IJRASET. URL: https://www.ijraset.com/research-paper/social-engineering-attacks-in-cybersecurity (дата звернення: 19.02.2026).
6. Людський фактор у фішингу: розуміння вразливості та стійкості. sciencedirect.com. URL: https://www.sciencedirect.com/science/article/abs/pii/S0920548925000431 (дата звернення: 19.02.2026).

Глущенко Аліна Вікторівна – студентка групи 1КІТС-24б кафедри менеджменту і безпеки інформаційних систем факультет менеджмент і інформаційна безпека, Вінницький національний технічний університет, Вінниця, gluschenko.a.278@gmail.com

Hlushchenko Alina Viktorivna – student of group 1KITS-24b, department of management and information systems security, faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, gluschenko.a.278@gmail.com