Перелік від 01.10.2025 № 1226 Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1226-2025-%D0%BF

9. Реформування адміністративних послуг: аналітичний матеріал. Київ : Лабораторія законодавчих ініціатив, 2024. URL: https://parlament.org.ua/wp-content/uploads/2024/12/ali_brief_adminservices.pdf

10. Recommendation CM/Rec(2007)7 of the Committee of Ministers to member states on good administration. Council of Europe, 2007. URL: https://rm.coe.int/cmrec-2007-7-of-the-cm-to-ms-on-good-administration/16809f007c

DOI https://doi.org/10.36059/978-966-397-550-4-60

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ІНСТРУМЕНТ КІБЕРЗЛОЧИНЦІВ: ШЛЯХИ ПРОТИДІЇ

Пліс Т. Ю.
здобувач
Одеський державний університет внутрішніх справ
м. Одеса, Україна
Науковий керівник: **Грезіна О. М.**
доктор філософії, доцент кафедри кримінального аналізу та інформаційного аналізу
Одеський державний університет внутрішніх справ
м. Одеса, Україна

Соціальна інженерія залишається одним із найефективніших інструментів кіберзлочинців, оскільки спрямована не на технічні вразливості систем, а на психологічні особливості людини. Кіберзлочинці використовують принципи маніпуляції, такі як авторитет, терміновість, страх, довіра та дефіцит, щоб змусити жертву самостійно надати доступ до інформації, виконати шкідливі дії чи розкрити конфіденційні дані [3]. У 2024–2025 роках соціальна інженерія стала домінуючим вектором початкового доступу в кібератаках, обійшовши традиційні технічні заходи захисту завдяки фокусу на людському факторі [1]. Згідно з даними, соціальна інженерія становила 36 % усіх інцидентів з початковим доступом у період з травня 2024 по травень 2025 року, причому значна частина атак була фінансово мотивованою [1].

Соціальна інженерія охоплює широкий спектр тактик: фішинг, претекстинг (створення вигаданих сценаріїв), baiting (приманка), vishing

(голосовий фішинг) та імперсонацію. У 2025 році спостерігається значне ускладнення методів завдяки інтеграції штучного інтелекту. З'явилися масові кампанії ClickFix, коли жертву обманом змушують вставити шкідливий код через фальшиві сповіщення браузера чи оновлення, що призводить до встановлення інфостілерів або RAT [1]. Інша поширена тактика – email bombing (масове підписування на спам), яка створює плутанину в поштовій скриньці, приховує справжні сповіщення MFA та відкриває шлях для подальшого vishing чи імперсонації через Teams [2].

AI значно посилює ефективність атак: генеруються deepfake-аудіо та відео для імітації керівників чи родичів, що експлуатує принципи авторитету та емоційного зв'язку. Наприклад, deepfake-голос CEO використовується для шахрайських переказів коштів, а синтетичні ідентичності дозволяють масштабувати атаки [3]. Фішинг залишається основним методом (65 % соціально-інженерних інцидентів), але доповнюється SEO-отруєнням, malvertising та device code phishing, який обходить MFA через підроблені OAuth-додатки [1; 2]. У 2025 році 66 % атак були спрямовані на привілейовані облікові записи, що призводило до швидкої ескалації привілеїв та викрадення даних у 60 % випадків [1].

Ефективна протидія вимагає комплексного підходу, що поєднує технічні, організаційні та людські заходи. По-перше, посилення людського фактора через регулярне навчання та симуляцію атак. Працівників слід навчати розпізнавати ознаки маніпуляції (терміновість, авторитет, неочікувані запити), перевіряти джерела інформації та уникати імпульсивних дій. Особлива увага – до розпізнавання deepfake та ClickFix [3; 1]. По-друге, технічні заходи: впровадження фішинг-стійкого MFA (блокує понад 99 % несанкціонованого доступу), моніторинг поведінки (UEBA, ITDR), блокування підозрілих скриптів, посилення браузерів та фільтрація DNS/URL [2; 1]. Важливо контролювати процеси відновлення ідентичності та обмежувати використання нативних інструментів (наприклад, Quick Assist чи RMM). По-третє, організаційні заходи: принцип Zero Trust, сегментація доступу, моніторинг ранніх індикаторів (credential harvesting, аномальна поведінка), а також участь у обміні розвідданими та створення планів реагування. Регуляторні ініціативи мають передбачати відповідальність платформ за запобігання зловживанню AI [2; 3].

Соціальна інженерія у 2025 році перетворилася на масштабовану, автоматизовану та фінансово орієнтовану загрозу, що використовує AI для обходу традиційних захисних механізмів. Основний шлях протидії – поєднання постійного підвищення обізнаності користувачів, впровадження поведінкового аналізу та Zero Trust-архітектури. Лише комплексний підхід, що враховує психологічні аспекти та технічні інновації, дозволить суттєво знизити ефективність таких атак [1; 2; 3].

Література:

1. Unit 42. 2025 Unit 42 Global Incident Response Report: Social Engineering Edition. Palo Alto Networks. 2025. URL: https://unit42.paloaltonetworks.com/2025-unit-42-global-incident-response-report-social-engineering-edition
2. Microsoft Digital Defense Report 2025. Microsoft Corporation, 2025. URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf
3. Benusi A. A Practical Analysis of Social Engineering Attacks and Countermeasures. *CEUR Workshop Proceedings*. 2025. Vol. 4044. URL: https://ceur-ws.org/Vol-4044/short02.pdf

DOI https://doi.org/10.36059/978-966-397-550-4-61

СПЕЦИФІКА ГЛОБАЛЬНИХ ЮРИДИЧНИХ МЕХАНІЗМІВ У ВИМІРІ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ ВІЙН

Кушнір В. В.
здобувач 3 курсу третього (освітньо-наукового) рівня вищої освіти доктора філософії,
спеціальності 293 «Міжнародне право»,
кафедри морського та міжнародного права
Міжнародний гуманітарний університет
м. Одеса, Україна

Аспекти системної протидії дезінформації та пропаганді у її різних форматах набуло для вітчизняної юридичної доктрини максимально гострих рис за умов масштабної російської агресії.

У відповідному контексті слід вказати на розвиток стандартів ООН у сфері протидії дезінформації у резолюції Ради Безпеки 2686 (2023) від 14 червня 2023 року, яка оцінює відповідні виклики насамперед у вимірі міжнародної безпеки, вказуючи на «випадки насильства, що підживлюється використанням мови ненависті, поширенням хибної інформації та дезінформацією, у тому числі у соціальних мережах», й на «жертви нетерпимості, дискримінації та підбурювання у ситуаціях збройного конфлікту», але з особливою увагою до «боротьби з дезінформацією та поширенням хибної інформації з метою зміцнення