Федорова Людмила Федорівна
Студентка групи 202_СПС ННІ права та психології НАВС

Науковий керівник:
Пакриш Олександр Євгенійович
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ВИКОРИСТАННЯ ЕМОЦІЙ ЛЮДИНИ ДЛЯ ВЧИНЕННЯ КІБЕРЗЛОЧИНІВ

У сучасному цифровому світі кіберзлочини стають дедалі витонченішими. Якщо раніше злочинці здебільшого використовували технічні методи злому систем, то сьогодні вони дедалі частіше звертаються до психологічних методів впливу на людину. Найефективнішим серед них є використання емоцій. Людські почуття – страх, довіра, співчуття, жадібність, цікавість – стають знаряддям злочину, яке дозволяє обійти навіть найсучасніші системи безпеки. Цей феномен отримав назву *соціальна інженерія* – це використання психологічних прийомів для маніпулювання людьми з метою отримання конфіденційної інформації або доступу до систем. Кіберзлочинці розуміють: у стані сильних емоцій люди частіше діють імпульсивно і рідше аналізують ситуацію. Вони не зважають на логіку чи перевірку фактів, а керуються почуттями. Тому злочинці створюють ситуації, що викликають емоційну напругу або, навпаки, приємне очікування вигоди. Основні емоції, які експлуатують злочинці:

1. ***Страх і паніка***. Найпоширеніша емоція, яку використовують для тиску.

Приклад: користувач отримує лист із нібито офіційного джерела – наприклад, «Ваш банківський рахунок буде заблоковано через підозрілу активність! Потрібно терміново підтвердити Вашу особу за посиланням»». Злякавшись, людина натискає на посилання і вводить свої дані – логін, пароль, номер картки. Так злочинці отримують доступ до її коштів. У цьому випадку страх паралізує критичне мислення: людина діє миттєво, щоб «уникнути небезпеки».

2. ***Співчуття і бажання допомогти***. Маніпуляції часто побудовані на людяності.

Приклад: зловмисник створює фейкову сторінку у соцмережі й поширює пости на кшталт: «Дитині терміново потрібна операція, допоможіть хто чим може». Люди, керуючись співчуттям, переказують гроші на картку, навіть не перевіряючи достовірність інформації. Подібні «емоційні пастки» особливо поширені у часи воєн, катастроф, коли емоційна напруга в суспільстві висока.

3. ***Жадібність і бажання швидкого прибутку***. Емоція вигоди часто приглушує обережність.

Приклад: користувач отримує повідомлення: «Ви стали переможцем лотереї Google! Для отримання призу введіть свої дані». Або ж – «Інвестуйте 1000 грн сьогодні й заробіть 10000 за тиждень». Очікування легкої вигоди змушує людину ігнорувати підозри.

4. ***Бажання дізнатися щось «таємне» або «сенсаційне»*** – ще один гачок.

Приклад: людині надсилають повідомлення: «Подивись, що про тебе написали!» або «Шокуюче відео твого знайомого». Відкриваючи посилання, користувач активує вірус або надає доступ до свого акаунта.

5. ***Почуття авторитету і довіри***. Злочинці часто видають себе за представників офіційних структур, банків, керівників або навіть знайомих.

Приклад: співробітник отримує лист нібито від директора компанії: «Терміново надішліть мені звіт і паролі до системи». Прагнучи виконати наказ керівництва, працівник не перевіряє справжність відправника.

Дослідження показують, що люди більш схильні піддаватися емоційним маніпуляціям у стані:

- втоми, коли увага розсіяна;
- стресу, коли знижується раціональне мислення;
- багатозадачності, коли одночасно потрібно вирішувати кілька питань;
- коли людина має низький рівень цифрової грамотності.

Крім того, деякі особистісні риси – наприклад, довірливість, відкритість, співчутливість – також підвищують ризик потрапити на гачок кіберзлочинців.

Приклади реальних випадків дії психологічних чинників вразливості:

1. “Love Scam” (романтичні шахрайства): злочинці знайомляться в соцмережах, вибудовують довіру, а потім просять гроші на «лікування», «переїзд» чи «візу». Жертви часто втрачають великі суми, бо керуються емоцією кохання та довіри.

2. “Фішинг” від імені банку: під час пандемії COVID-19 тисячі людей отримали листи про нібито фінансову допомогу від банків. Натиснувши на фальшиве посилання, вони передавали свої дані шахраям.

3. Соціальні мережі: зловмисники використовують фейкові сторінки відомих благодійних фондів, які викликають довіру, і збирають пожертви для власної вигоди.

Наслідки таких злочинів можуть бути дуже серйозними:

- Фінансові втрати – від кількох сотень до мільйонів гривень.
- Витік персональних даних – доступ до паролів, фото, листування.
- Емоційна травма жертви – почуття провини, сором, недовіра до оточення.
- Репутаційні збитки – особливо для організацій і компаній.

Шляхи захисту від кіберзлодіїв:

1. *Розвивати емоційну обізнаність*. Якщо повідомлення викликає сильну емоцію – страх, злість, азарт чи співчуття – це сигнал бути обережним.

2. *Зробити паузу*. Не приймати жодних рішень одразу, особливо якщо вас підганяють словами «терміново».

3. *Перевіряти джерело інформації*. Телефонувати або писати офіційним контактам замість натискання на сумнівні посилання.

4. *Підвищувати цифрову грамотність*. Знання про фішинг, шкідливі сайти, конфіденційність допомагають уникнути маніпуляцій.

5. *Психологічна стійкість*. Людина, яка розуміє власні емоційні реакції, рідше стає жертвою маніпуляцій.

Висновки. Використання емоцій у кіберзлочинності – це приклад того, як психологія може стати зброєю в руках маніпулятора. Емоції – це природна і важлива частина людського життя, але саме вони можуть зробити нас вразливими.

Знання власних реакцій, розвиток критичного мислення і цифрової культури – це головні засоби захисту у світі, де замість фізичних грабіжників з'явилися емоційні хакери.

Список використаних джерел:

1. Schmitt, Marc, and Ivan Flechais. 2024. *Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing.* Artificial Intelligence Review 57: Article 324. https://doi.org/10.1007/s10462-024-10973-2.

2. Europol. 2024. *Internet Organised Crime Threat Assessment (IOCTA) 2024.* The Hague: Europol. PDF. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

3. National Cyber Security Centre (NCSC). 2024. *NCSC Annual Review 2024.* London: NCSC. PDF. https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf.

4. Sandoval, María Paz, Maria de Almeida Vau, John Solaas, and Luano Rodrigues. 2024. "Threat of Deepfakes to the Criminal Justice System: A Systematic Review." *Crime Science* 13 (1): 41. https://doi.org/10.1186/s40163-024-00239-1.

5. Wiemken, Mika, Kilian Hildebrandt, André Jeworutzki, and Larissa Putzar. 2025. "Emotional Manipulation in Phishing Emails: Experimental Study of Affective Responses and Human Classification Errors in a Simulated Email Environment." Proceedings / Publication record (ACM / conference paper; Hamburg University of Applied Sciences). DOI/ACM record: https://doi.org/10.1145/3733155.3736796

6. Wu, Jie. 2024. "Social and Ethical Impact of Emotional AI Advancement: The Rise of Pseudo-Intimacy Relationships and Challenges in Human Interactions." *Frontiers in Psychology* 15:1410462. https://doi.org/10.3389/fpsyg.2024.1410462.

7. Balcombe, Luke. 2025. "The Mental Health Impacts of Internet Scams." *International Journal of Environmental Research and Public Health* 22, no. 6: 938. https://doi.org/10.3390/ijerph22060938.

8. Espinoza, Michelle. 2024. *Weaponization of Conscience in Cybercrime and Online Fraud: A Novel Systems Theory.* arXiv preprint arXiv:2403.14667. https://arxiv.org/abs/2403.14667.

9. “A Comprehensive Survey on Social Engineering-Based Attacks on Social Networks.” 2024. *International Journal / IJAAS (online)* — A comprehensive review article (systematic survey; PDF available). https://www.science-gate.com/IJAAS/Articles/2024/2024-11-04/1021833ijaas202404016.pdf.

10. Tóth, R., et al. 2024. “Impact of Emotions on User Behavior Toward Phishing Emails.” *Nordic Institute for Knowledge and Technology (NIKT) / NTNU open journal* (conference/journal item). PDF available from NTNU repository. https://www.ntnu.no/ojs/index.php/nikt/article/view/6243 .

Слєпко Ангеліна Іванівна
Студентка групи 202_СПС ННІ права та психології НАВС

Науковий керівник:
Пакриш Олександр Євгенійович
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій ННІ права та психології НАВС

ВІКОВІ ТА ГЕНДЕРНІ ВІДМІННОСТІ В ДОВІРЛИВОСТІ ДО ОНЛАЙН-ПРОПОЗИЦІЙ ЯК ФАКТОР РИЗИКУ ДО КІБЕРШАХРАЙСТВА

У сучасному цифровому середовищі кількість користувачів Інтернету стрімко зростає, що, з одного боку, відкриває нові можливості для спілкування, роботи й навчання, а з іншого – створює нові загрози. Однією з найпоширеніших небезпек є *кібершахрайство* – комплекс дій, спрямованих на отримання особистих даних, грошей чи доступу до конфіденційної інформації. Одним із ключових чинників, що визначає ймовірність стати жертвою кібершахрайства, виступає довірливість до онлайн-пропозицій. Довірливість у цьому контексті розуміється як схильність приймати інформацію або пропозицію без достатньої перевірки її достовірності.

Актуальність теми полягає в тому, що рівень довірливості значною мірою залежить від індивідуально-психологічних особливостей людини, зокрема від її віку та гендерної належності. Дослідження показують, що вікові зміни когнітивних функцій, емоційна вразливість і соціальна ізоляція можуть підвищувати рівень довірливості серед літніх осіб [1, с. 4]. Водночас молодь, попри високий рівень технічної грамотності, часто переоцінює свої навички розпізнавання шахрайства, що також створює ризик стати жертвою.