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.

Тему довіри в Інтернет-середовищі, вікових та гендерних особливостей сприйняття ризику активно вивчають: Н. М. Василець – досліджує соціально-психологічні чинники довіри громадян в умовах цифровізації [2]; О. М. Мосол – аналізує психологічні аспекти міжособистісної довіри та її роль у взаємодії людей [3]. Зарубіжні автори, зокрема D. Modic і M. Anderson, досліджують когнітивні та емоційні механізми, які роблять людей більш сприйнятливими до шахрайських повідомлень [4].

В межах гендерного аспекту науковці звертають увагу, що чоловіки й жінки по-різному оцінюють ступінь ризику та довіри до джерел інформації. Наприклад, жінки частіше довіряють відгукам, емоційним повідомленням та соціальним рекомендаціям, тоді як чоловіки – інформації, яка виглядає логічно структурованою чи офіційною. У роботі Rebecca Cole [5, с. 3] наголошується, що самотність і прагнення до соціального контакту підсилюють довірливість жінок у випадках онлайн-знайомств, що призводить до зростання кількості романтичних шахрайств.

Як показує дослідження Chen H. та співавторів, літні користувачі мережі частіше піддаються на шахрайські схеми, пов’язані зі здоров’ям, оскільки мають обмежену цифрову компетентність і схильні довіряти повідомленням, які апелюють до страху за власний добробут. У той же час молоді люди є вразливими до фінансових ігор, інвестиційних пропозицій або швидких заробітків, що базуються на довірі до “молодіжних” брендів і популярних блогерів.

Вікові відмінності також впливають на емоційну складову сприйняття інформації. Літні особи демонструють нижчу здатність до критичної оцінки контенту, часто сприймають повідомлення буквально та покладаються на попередній життєвий досвід, який не завжди адаптований до цифрового середовища. Як зазначено у звіті MDPI [6], з віком знижується здатність розрізняти безпечні й шкідливі повідомлення, що збільшує ризик стати жертвою фішингу.

Гендерні відмінності проявляються і в особистісних якостях, що визначають ступінь довірливості. Жінки схильні виявляти більше емпатії та відкритості до міжособистісних контактів, що може збільшувати ризик під час онлайн-спілкування. Чоловіки, навпаки, часто демонструють надмірну впевненість у власній цифровій компетентності, через що ігнорують попереджувальні сигнали шахрайства

Типи онлайн-пропозицій, що найчастіше стають інструментами шахрайства, охоплюють кілька категорій: медичні та оздоровчі поради, пропозиції швидкого заробітку, онлайн-знайомства, “акційні” покупки, розіграші, а також запрошення до сумнівних фінансових проєктів. Для кожної вікової та гендерної групи шахраї створюють окремі тактики маніпуляції. Наприклад, для літніх – через емоційні повідомлення (“Ви виграли приз” або “Терміново потрібно оновити дані банку”), для молоді – через цікаві виклики, “прибуткові інвестиції” або псевдопартнерства.

Психологічними чинниками підвищеної довірливості є низький рівень критичного мислення, потреба у визнанні, відчуття самотності, а також відсутність навичок перевірки джерел. Вік і гендер лише підсилюють ці механізми, створюючи специфічний профіль потенційної жертви. Як зазначає Cole [5, с. 4], “самотність і віра в щирість іншої людини в онлайні часто є тим самим гачком, який призводить до фінансових і емоційних втрат”.

З огляду на викладене, для зниження ризику потрапляння в пастку кібершахрайства доцільно дотримуватися *низки загальних порад*. Насамперед, слід розвивати критичне мислення та навички перевірки достовірності онлайн-інформації. Важливо не реагувати імпульсивно на емоційні або “термінові” повідомлення, уникати розголошення особистих і фінансових даних, а також перевіряти джерело будь-яких пропозицій. Рекомендується використовувати складні паролі, двофакторну автентифікацію та регулярно оновлювати програмне забезпечення. Особливу увагу варто приділяти підвищенню цифрової грамотності літніх користувачів і формуванню у молоді звички критично оцінювати онлайн-контент. Для жінок важливо зберігати обережність у випадках емоційних або соціально орієнтованих пропозицій, а чоловікам – уникати надмірної самовпевненості у власних технічних навичках.

Висновки. Довірливість до онлайн-пропозицій є одним із ключових психологічних чинників, що підвищують ризик стати жертвою кібершахрайства. Вікові та гендерні особливості користувачів суттєво впливають на рівень цієї довірливості: літні люди частіше демонструють емоційну вразливість і знижену критичність сприйняття інформації, тоді як молодь нерідко переоцінює власну цифрову компетентність. Гендерні відмінності проявляються у різних формах довіри до джерел – емоційній у жінок та раціональній у чоловіків. Отже, ефективна профілактика кібершахрайства потребує диференційованого підходу: розвитку цифрової грамотності серед літніх осіб, формування критичного мислення у молоді та підвищення емоційної стійкості в усіх групах користувачів. Підвищення обізнаності й уважності в онлайн-середовищі є запорукою безпечного цифрового простору.

Список використаних джерел:

1. Chen H., He M., Xu X., Atkin D. Examining older adults’ vulnerability to online health scams: insights from routine activity theory // *Frontiers in Public Health*. – 2025.

2. Василець Н. М. Соціально-психологічні чинники довіри громадян в умовах цифровізації: дис. канд. психол. наук. – Київ: ІПЗД НАПН України, 2021. – 201 с.

3. Мосол О. М. Психологічні аспекти міжособистісної довіри. – *Науковий вісник Ужгородського університету. Серія: Психологія*, 2019. – Вип. 1(44). – С. 49–54.

4. Modic, D., Anderson, R. Reading this may harm your computer: The psychology of scams. – *Journal of Cybersecurity*, 2015. – Vol. 1(1). – P. 87–97.

5. Cole R. Scammed by Love: The Role of Loneliness, Trust, and Age in Financial Losses from U.S. Online Romance Scams // *Innovation in Aging*. – 2024.

6. Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review // *MDPI*. – 2022. – Vol. 15(4), p. 2236.

Гуменюк Вікторія Олегівна
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

ЗНАЧЕННЯ ЛЮДСЬКОГО ФАКТОРУ У КІБЕРБЕЗПЕЦІ

У сучасному світі, де більшість інформаційних процесів відбувається у цифровому просторі, питання кібербезпеки набуває вирішального значення. Ми живемо в епоху, коли інформація стала не лише ресурсом, а й об'єктом постійних атак. Щодня відбуваються мільйони кібератак на приватні особи, підприємства й навіть державні установи. Попри стрімкий розвиток технологій захисту – антивірусів, систем виявлення вторгнень, шифрування даних, – головним і найвразливішим елементом системи безпеки залишається людина. Саме людський фактор, тобто дії, помилки чи поведінкові особливості користувачів, визначає, наскільки ефективною буде будь-яка система кіберзахисту.

Людський фактор у кібербезпеці – це сукупність психологічних, поведінкових і організаційних аспектів, які впливають на безпеку інформаційних систем. Іншими словами, це все, що пов'язано з тим, як люди взаємодіють із технологіями.

Людина може бути як найсильнішою, так і найслабшою ланкою в системі. З одного боку, жодна система не може ефективно працювати без відповідальних і навчених працівників. З іншого – саме через необережність, неуважність або навмисні дії люди часто виникають серйозні порушення безпеки.

Помилки користувачів є однією з найпоширеніших причин кіберінцидентів. Наприклад, відкриття шкідливих файлів, натискання на підозрілі посилання, введення паролів на фішингових сайтах або ненавмисне розголошення конфіденційних даних.