УДК 004.056.5:316.77

https://doi.org/10.52058/3041-1793-2025-11(16)-95-104

Габорець Ольга Андріївна доктор філософії, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, м. Кропивницький, https://orcid.org/0000-0001-7791-6795

Лунгол Ольга Миколаївна кандидат педагогічних наук, доцент, завідувач кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, м. Кропивницький, https://orcid.org/0000-0001-8128-0072

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ФЕНОМЕН ІНФОРМАЦІЙНОГО ВПЛИВУ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Анотація. У статті здійснено комплексне дослідження соціальної інженерії як феномену інформаційного впливу в умовах цифровізації суспільства. Визначено, що соціальна інженерія є міждисциплінарним явищем, яке поєднує технічні, психологічні, когнітивні та комунікативні механізми маніпулювання поведінкою людини. Доведено, що людський фактор залишається найуразливішим елементом кібербезпеки, оскільки більшість користувачів приймають рішення під дією емоційних і когнітивних спрощень, що створює сприятливі умови для експлуатації довіри. Проаналізовано ключові психологічні тригери – ефекти авторитету, дефіциту, терміновості й соціального підтвердження, які формують поведінкову вразливість особи. Наведено приклади фішингових і соціоінженерних атак у месенджерах Telegram та Viber, де поєднано психологічні стимули й технологічні інструменти для створення ефекту достовірності. Обґрунтовано роль OSINT-технологій, аналітики даних і штучного інтелекту у створенні персоналізованих сценаріїв впливу, що сприяють виникненню феномену «алгоритмічного управління довірою». Зазначено, що соціальна інженерія в умовах гібридної війни використовується як інструмент когнітивного тиску та дестабілізації суспільної свідомості. Відсутність нормативного визначення цього поняття у правовому полі України ускладнює кваліфікацію подібних злочинів, що потребує удосконалення національної системи протидії. Наголошено на важливості розвитку інформаційної культури, критичного мислення, медіаграмотності й цифрової етики як основи формування когнітивного імунітету користувачів до маніпулятивних впливів. Доведено,

що інтеграція технічних, освітніх, правових і культурних підходів є ключовою умовою побудови ефективної моделі кіберзахисту в сучасному інформаційному середовищі.

Ключові слова: соціальна інженерія, інформаційний вплив, людський фактор, когнітивні упередження, OSINT, інформаційна культура, цифрове середовище, кібербезпека.

Haborets Olha PhD in Pedagogical Sciences, Docent, Associate Professor of the Department of Operational-Search Activity and Information Security of the Educational and Scientific Institute for the Training of Specialists for Criminal Police Units named after E.O. Didorenko of Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0000-0001-7791-6795

Lunhol Olha PhD in Pedagogical Sciences, Docent, Head of the Department of Operational-Search Activity and Information Security of the Educational and Scientific Institute for the Training of Specialists for Criminal Police Units named after E.O. Didorenko of Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0000-0001-8128-0072

SOCIAL ENGINEERING AS A PHENOMENON OF INFORMATION INFLUENCE IN THE DIGITAL ENVIRONMENT

Abstract. The article provides a comprehensive study of social engineering as a phenomenon of informational influence in the context of digital transformation. Social engineering is defined as an interdisciplinary construct that integrates technical, psychological, cognitive, and communicative mechanisms of behavioral manipulation. The research proves that the human factor remains the most vulnerable element of cybersecurity, as most user decisions are driven by emotions and cognitive shortcuts, making trust a primary target of exploitation. The study identifies key psychological triggers – authority, scarcity, urgency, and social proof – that shape behavioral vulnerability and facilitate manipulation. Examples of phishing and socio-engineering attacks in Telegram and Viber are analyzed, demonstrating the synthesis of emotional stimulation with technological tools that create an illusion of credibility. The role of OSINT technologies, data analytics, and artificial intelligence is substantiated in designing personalized influence scenarios, giving rise to the phenomenon of “algorithmic trust management”. The article highlights that, within hybrid warfare, social engineering functions as an instrument of cognitive pressure and informational destabilization of public perception. The absence of a precise legal definition of “social engineering” in Ukrainian law complicates the prosecution of related offenses, necessitating the refinement of the national counteraction framework. Emphasis is placed on the development of information culture, critical thinking, media literacy, and digital ethics as the

foundation of users' cognitive immunity to manipulative influences. The study concludes that only the integration of technical, educational, legal, and cultural strategies can ensure an effective model of cybersecurity in the contemporary information environment.

Keywords: social engineering, informational influence, human factor, cognitive biases, OSINT, information culture, digital environment, cybersecurity.

Постановка проблеми. Активний розвиток цифрових технологій та зростання ролі інформаційного простору у суспільному житті зумовили появу нових форм впливу на свідомість і поведінку людини. Одним із найнебезпечніших проявів цього процесу є соціальна інженерія – цілеспрямований вплив на особу з метою отримання вигоди або доступу до інформаційних ресурсів шляхом маніпулювання психологічними, когнітивними та комунікативними механізмами. Проблематика соціоінженерних атак набуває особливої актуальності в умовах гібридних інформаційних загроз, спрямованих не лише на окремих користувачів, а й на стратегічні інститути держави. Людський фактор при цьому виступає як найслабша, але водночас і найскладніша для захисту ланка інформаційної безпеки. Питання вивчення закономірностей соціальної інженерії в цифровому середовищі є важливим для розроблення ефективних систем протидії кіберзагрозам, формування інформаційної культури та підвищення когнітивної стійкості користувачів.

Аналіз останніх досліджень і публікацій. Проблема соціальної інженерії, як форми інформаційного впливу, привертає увагу науковців різних галузей – від інформаційної безпеки до психології комунікації. У працях О. Є. Зіменка підкреслюється міждисциплінарний характер соціальної інженерії як феномена, що інтегрує технологічні, соціально-психологічні та комунікативні складові інформаційного впливу. Учений визначає її як процес конструювання поведінкових рішень особи в умовах штучно сформованого інформаційного середовища [2]. У дисертаційному дослідженні О. В. Пугачова [3] висвітлено концепцію безпеки інформаційного простору держави, у межах якої соціальна інженерія розглядається як інструмент підриву інформаційного суверенітету через маніпулятивні технології. Наукові напрацювання сучасних авторів у сфері кібербезпеки зосереджені на дослідженні психологічних тригерів, алгоритмів фішингових атак, аналізі поведінкових шаблонів користувачів та застосуванні OSINT-технологій у контексті протидії соціоінженерним впливам.

Проведений огляд [1 – 5] свідчить, що попри наявність значної кількості публікацій, залишається недостатньо розкритим питання взаємозв'язку між когнітивними особливостями користувача, алгоритмічним управлінням інформаційними потоками та сучасними інструментами соціальної інженерії. Це визначає актуальність подальшого дослідження феномену соціальної інженерії в контексті розвитку цифрового середовища, його ролі в інформаційній безпеці особи, суспільства й держави.

Метою статті є дослідження соціальної інженерії як феномену інформаційного впливу в цифровому середовищі, з'ясування її механізмів, технологічних і психологічних інструментів реалізації, а також визначення шляхів підвищення ефективності протидії цьому явищу через розвиток інформаційної культури та когнітивної стійкості користувачів.

Виклад основного матеріалу. Соціальна інженерія постає сьогодні не лише як набір технік кіберзлочинців, а і як складний соціально-технологічний феномен, що інтегрує у собі психологічні механізми впливу, алгоритмічне управління довірою, когнітивні моделі поведінки та інформаційно-комунікаційні технології. Вона є перехрестям гуманітарних і технічних наук, де психологічна вразливість людини використовується як канал несанкціонованого доступу до інформаційних ресурсів або як інструмент прихованого керування поведінкою. Сучасна соціальна інженерія – це не просто спроба обману; це інтелектуально вибудувана система управління довірою, в якій знання з нейропсихології, лінгвістики, аналізу даних і штучного інтелекту поєднуються в єдину технологію інформаційного впливу.

Розвиток соціальної інженерії в цифровому просторі зумовлений масштабною цифровізацією суспільства, переходом комунікацій у середовище соціальних мереж і месенджерів, розширенням меж штучного інтелекту та автоматизованих алгоритмів рекомендацій. Людська свідомість, перевантажена інформаційними потоками, дедалі частіше приймає рішення нераціонально, під дією емоційних тригерів, що відкриває широкі можливості для маніпуляції. Соціальна інженерія діє не стільки через примус, скільки через формування контексту – створення ситуації, у якій користувач добровільно робить вигідний для зловмисника крок. У цьому сенсі вона є проявом сучасного типу влади – влади через інформаційні стимули, через структуровану присутність у цифровому середовищі.

Теоретично феномен соціальної інженерії слід розглядати у трьох вимірах. Перший – когнітивно-психологічний, що пояснює, чому люди схильні до довіри та як емоційні реакції впливають на обробку інформації. Другий – комунікативно-інформаційний, який охоплює архітектуру цифрових платформ, алгоритми рекомендацій, соціальні зв'язки, через які поширюються повідомлення. Третій – технологічний, що включає автоматизовані системи збору та обробки даних, штучний інтелект, аналітику поведінки, OSINT-модулі, які дозволяють зловмисникам прогнозувати реакції користувачів. Сукупно ці рівні формують механізм, у якому довіра стає технічно керованим ресурсом.

У сучасній парадигмі кібербезпеки соціальна інженерія розглядається як найслабша, але й найнебезпечніша ланка – людський фактор. На відміну від технічних компонентів інформаційних систем, які можна захистити через шифрування, автентифікацію чи багаторівневі протоколи, людська поведінка залишається найменш передбачуваним і найважче контрольованим елементом. Більшість рішень приймаються на основі інтуїції, а не раціонального аналізу. Саме ці інтуїтивні реакції і є мішенню соціального інженера. Використовуючи евристики, ефект терміновості, дефіциту, соціального підтверд-

ження або авторитету, зловмисник створює ситуацію, коли користувач сам ініціює небезпечну дію – переходить за посиланням, вводить дані, підтверджує платіж тощо. В умовах цифрового шуму, постійного потоку повідомлень і фрагментованої уваги, ймовірність такої поведінки зростає в геометричній прогресії.

Особливої небезпеки соціальна інженерія набуває у просторі соціальних мереж і месенджерів – таких як Telegram і Viber, де довіра підкріплюється відчуттям приватності, а поширення контенту має вірусний характер. Тут соціоінженерні атаки поєднують психологічну маніпуляцію з технологічним фішингом. Зловмисники створюють канали, що імітують офіційні сторінки міжнародних організацій, банків, благодійних фондів, державних структур. Мета – викликати емоційне залучення, використати довіру та спонукати людину до дії, зокрема – натискання на фішингове посилання.

Показовим є приклад поширення у 2024–2025 роках повідомлень у Telegram, які нібито інформують про виплату грошової допомоги від ООН. На одному з таких повідомлень (рис. 1) зображено офіційний логотип ООН, жовто-блакитне тло, символ серця, що асоціюється з благодійністю, і текст: «Стартувала виплата 6600 грн: українці можуть отримати від ООН нову грошову допомогу». Використовується типова фраза соціальної інженерії – «інструкцію завантажили тут», що супроводжується гіперпосиланням на фішинговий сайт. Візуальна стилізація імітує офіційний стиль міжнародних організацій, а текстовий компонент активує когнітивні тригери – емоцію надії, терміновість дії, довіру до авторитету. Такі повідомлення масово поширюються бот-мережами, які експлуатують ефект групової довіри – чим більше реакцій, тим легше переконати наступних користувачів у достовірності інформації.

Рис. 1. Приклад імітації повідомлення про «допомогу від ООН» у Telegram-каналі з фішинговим посиланням (анонімізовано)

Не менш показовим є випадок поширення фейкових повідомлень у Viber, де соціальна інженерія поєднується з персоніфікацією. На зображенні (рис. 2) видно, як користувачеві надходить повідомлення від особи на ім'я Анна: «Сьогодні отримали допомогу від Червоного Хреста, прийшли на ОщадБанк 9600 грн, спробуйте, поки є можливість». Посилання веде на фішинговий сайт, створений на платформі tilda.ws, що дозволяє швидко виготовляти копії офіційних сторінок. Структура повідомлення побудована за всіма законами когнітивного впливу: створення ефекту достовірності (згадка банку та конкретної суми), емоційного заохочення (інтонація радості й довіри), соціального доказу («ми думали, що брехня, а в результаті виплатили»), підкріплення візуальним елементом – зображенням автомобіля Червоного Хреста.

Ці приклади демонструють, що соціальна інженерія у цифровому середовищі є технологічно вибудуваним процесом керування емоційним станом користувача. Вона спирається на три ключові елементи: довіру до авторитету (ООН, Червоний Хрест), страх втрати можливості (ефект дефіциту) та групове наслідування (ефект соціального підтвердження). Коли ці фактори поєднуються, навіть користувач із базовими знаннями безпеки часто не встигає здійснити критичну оцінку.

Рис. 2. Приклад фішингового повідомлення у Viber під виглядом звернення від Червоного Хреста (анонімізовано)

Ще одним різновидом соціоінженерних повідомлень є використання так званих «емоційних пасток», які базуються не на обіцянці матеріальної вигоди, а на провокуванні шоку, страху або цікавості. На зображенні (рис. 3) наведено типовий приклад повідомлення з месенджера, яке містить елемент візуального попередження – червоний знак оклику у колі, що сприймається як символ небезпеки, терміновості та ексклюзивності інформації. Текст повідомлення побудований за принципом емоційного стимулу: «Ви тільки подивіться, що вони сьогодні накоїли! Шокуючі кадри з Кропивницького від свідків!» – із подальшим закликом перейти за посиланням для перегляду відео. Ця конструкція одночасно активує кілька когнітивних механізмів: ефект страху втратити важливу інформацію, емоційну реакцію на сенсаційність і рефлекс довіри до «свідків», тобто до «очевидців події». З технічного боку такі повідомлення часто ведуть на фішингові або шкідливі ресурси, які збирають дані про користувача або інфікують пристрій. У психологічному вимірі це форма примусу через емоцію: користувач не встигає критично оцінити ситуацію, адже його увагу спрямовано на сенсаційність і тривогу. У результаті емоційна активація стає інструментом управління поведінкою. Цей приклад демонструє, що сучасна соціальна інженерія не обмежується економічними мотивами чи імітацією офіційних структур, а активно використовує когнітивно-емоційні механізми масової комунікації для стимулювання неконтрольованої реакції.

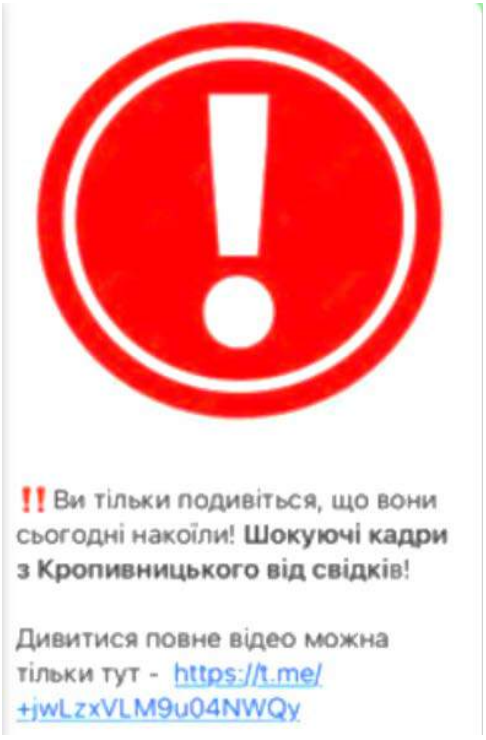

Рис. 3. Приклад соціоінженерного повідомлення з елементами шокового контенту у месенджері (анонімізовано)

Для аналізу подібних явищ OSINT-технології відіграють вирішальну роль. Вони дозволяють ідентифікувати джерела, відстежувати доменні реєстрації, часові збіги, спільні сервери, визначати повторювані стилістичні шаблони. Такі методи дають змогу фахівцям CERT-UA та кіберпідрозділам СБУ фіксувати цілі кампанії інформаційного впливу, що синхронізуються з певними соціальними чи політичними подіями. Аналіз телеграм-каналів, бот-мереж, шаблонів мови повідомлень і структури URL-посилань розкриває координовані схеми поширення дезінформації, які часто мають геополітичний підтекст.

Соціальна інженерія у гібридній війні є особливо небезпечним інструментом. Її завдання полягає не лише у викраденні даних, а й у дестабілізації емоційного стану населення, формуванні атмосфери недовіри, паніки або фаталізму. Поширення фейкових повідомлень про «масові виплати», «мобілізації», «втечу керівництва», «крах банків» тощо – це приклади когнітивних атак, спрямованих на підрив інформаційної стійкості. Тут соціальна інженерія поєднується з інформаційно-психологічними операціями, які мають чітко визначені цілі та координуються через соціальні медіа.

Паралельно спостерігається поява нової тенденції – автоматизованих систем маніпулювання довірою. Завдяки штучному інтелекту соціоінженерні повідомлення можуть створюватися й адаптуватися в реальному часі. Моделі мовного аналізу, здатні відтворювати індивідуальний стиль користувача, формують персоналізовані повідомлення, які підвищують імовірність реакції. Так виникає феномен «алгоритмічного управління довірою»: поведінка користувача прогнозується, а сам користувач перетворюється на об’єкт безперервного спостереження та корекції.

У правовому вимірі соціальна інженерія залишається складною для класифікації. Українське законодавство містить низку актів, що побічно регулюють питання кіберзахисту – зокрема Закон України «Про основні засади забезпечення кібербезпеки України» [6] та Закон «Про захист персональних даних» [7]. Проте поняття соціальної інженерії не має чіткої нормативної дефініції, що ускладнює притягнення до відповідальності за подібні дії. Міжнародні стандарти ЄС, зокрема рекомендації ENISA, пропонують ширше тлумачення, у якому соціальна інженерія розглядається як частина ландшафту загроз поряд із фішингом, BEC-шахрайством і deepfake-маніпуляціями. Розробка національної методології класифікації таких злочинів є актуальним завданням для України у контексті євроінтеграції та побудови цифрової довіри.

В етичному аспекті соціальна інженерія також викликає низку дилем. З одного боку, вона використовується у кіберзлочинності для обману, з іншого – у навчанні та тренінгах з безпеки як засіб підвищення стійкості користувачів. Етичні фішингові кампанії дозволяють виявляти слабкі місця у поведінці працівників організацій, формуючи навички критичного мислення. Однак

межа між навчанням і маніпуляцією тут дуже тонка. Тому важливо, щоб будь-які освітні практики базувалися на принципах прозорості, інформованої згоди й неприпустимості психологічного тиску.

Культурна складова протидії соціальній інженерії полягає у формуванні глибинної цифрової етики, заснованої на принципах відповідальності, усвідомленості та критичної рефлексії. Йдеться не лише про набір правил кібергігієни, а про становлення нової системи цінностей, де інформація сприймається не як нейтральний ресурс, а як фактор впливу, що може як підсилювати, так і руйнувати соціальну довіру. У цьому контексті цифрова етика стає не лише інструментом самозахисту, а й елементом громадянської культури, що формує стійкість особистості до маніпуляцій у цифровому просторі. Усвідомлення природи інформаційних ризиків, розвиток аналітичного мислення, вміння розпізнавати емоційні тригери та штучні інформаційні конструкції – це ті компетентності, які мають формуватися системно, починаючи з освітнього процесу.

Сучасні освітні програми у сфері кібербезпеки мають поєднувати технічну підготовку з гуманітарним компонентом, що включає етичні та психологічні аспекти поведінки в мережі. Таке міждисциплінарне навчання сприяє розвитку критичного мислення, здатності самостійно оцінювати достовірність інформації, аналізувати джерела та виявляти приховані механізми впливу. Особливу роль тут відіграє медіаосвіта, яка навчає не просто «споживати» контент, а розуміти його структуру, цілі, маніпулятивні техніки й когнітивні ефекти.

Цифрова культура безпеки повинна включати не лише індивідуальні навички – такі як регулярне оновлення паролів, обережність із посиланнями, уважність до стилістики повідомлень або верифікація джерел, – але й колективну практику інформаційної взаємодії. В умовах гібридної війни, коли маніпуляції набувають системного характеру, саме культура взаємної обережності та довіри у цифрових спільнотах може слугувати запобіжником поширення дезінформації.

Формування культури протидії соціальній інженерії передбачає також розвиток внутрішньої когнітивної рівноваги – здатності зберігати емоційну стійкість перед інформаційними подразниками. Людина, яка усвідомлює принципи маніпулятивних стратегій, менш схильна до емоційних реакцій і більш готова до раціонального аналізу. Тому підвищення інформаційної грамотності має супроводжуватися формуванням психологічної саморегуляції, що дозволяє протистояти інформаційному тиску.

Висновки. Підсумовуючи, слід наголосити, що соціальна інженерія є системним феноменом сучасного інформаційного суспільства, який трансформується разом із розвитком технологій. Вона одночасно відображає і технічний прогрес, і психологічну вразливість людини. Протидія їй вимагає синергетичного підходу, що об’єднує науковий аналіз, міждисциплінарну

співпрацю, державну політику, правове регулювання та етичну освіту. Формування культури довіри, стійкості до інформаційного впливу та розуміння механізмів когнітивних маніпуляцій є основою національної кібербезпеки в умовах цифрової війни.

Література:

1. Габорець О., Чернобров В. Social engineering as a means of influence on people consciousness // Детермінанти посилення ролі освіти у повоєнному відновленні України: Березневий науковий дискурс 2023 : Міжнар. наук.-практ. конф. для освітян (м. Чернігів, 22 березня 2023 р.). – Чернігів : ГО «Науково-освітній інноваційний центр суспільних трансформацій», 2023. – С. 204–205.
2. Зіменко О. Є. Феномен інформаційного впливу у науковому середовищі: теорії, дефініції // Бібліотекознавство. Документознавство. Інформологія. – 2022. – № 1. – С. 90–97. – DOI: 10.32461/2409-9805.1.2022.257331
3. Пугачов О. В. Концептуальні засади забезпечення інформаційної безпеки держави в умовах гібридних загроз : дис. ... д-ра техн. наук : 21.05.01 – інформаційна безпека держави/ Олександр Вікторович Пугачов. – Київ : Національний університет оборони України імені Івана Черняховського, 2021. – 315 с.
4. Волобоєв А. О. Розвиток цифрової компетентності майбутніх фахівців юридичного спрямування: практичні аспекти / А. О. Волобоєв, О. М. Лунгол, О.А. Габорець // Вісник науки та освіти: журнал. 2022. № 5(5) 2022. – С. 193-204.
5. Жмурко О.І. Соціальна інженерія як загроза кібербезпеці: методи запобігання та захисту / О.І. Жмурко // Педагогіка безпеки. – № 9(1), С. 37–42. https://doi.org/10.31649/2524-1079-2024-9-1-037-042

References:

1. Haborets, O., & Chernobrov, V. (2023). Social engineering as a means of influence on people consciousness. In *Determianty posylennia roli osvity u povoyennomu vidnovlenni Ukrainy: Bereznevyi naukovyi dyskurs 2023 : Mizhnar. nauk.-prakt. konf. dlia osvitian (m. Chernihiv, 22 bereznia 2023 r.)* [Determinants of strengthening the role of education in the post-war recovery of Ukraine: March scientific discourse 2023 : International scientific and practical conference for educators (Chernihiv, March 22, 2023)] (pp. 204–205). Chernihiv: NGO «Scientific and Educational Innovation Center for Social Transformations» [in English].
2. Zimenko, O.Ye. (2022). Fenomen informatsiinoho vplyvu u naukovomu seredovyshchi: teorii, definitsii [The phenomenon of information influence in the scientific environment: theories, definitions]. *Bibliotekoznavstvo. Dokumentoznavstvo. Informolohiia – Library Science. Document Science. Informology, 1,* 90–97. https://doi.org/10.32461/2409-9805.1.2022.257331 [in Ukrainian].
3. Puhachov, O.V. (2021). Kontseptualni zasady zabezpechennia informatsiinoi bezpeky derzhavy v umovakh hibrydnykh zahroz [Conceptual foundations of ensuring state information security in conditions of hybrid threats] (Doctoral thesis, National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine). Retrieved from *National Defence University of Ukraine named after Ivan Cherniakhovskyi* [in Ukrainian].
4. Voloboiev, A.O., Lunhol, O.M., & Haborets, O.A. (2022). Rozvytok tsyfrovoi kompetentnosti maibutnikh fakhivtsiv yurydychnoho spriamuvannia: praktychni aspekty [Development of digital competence of future legal specialists: practical aspects]. *Visnyk nauky ta osvity: zhurnal – Bulletin of Science and Education: Journal*, *5*(5), 193–204 [in Ukrainian].
5. Zhmurko, O.I. (2024). Sotsialna inzheneriia yak zahroza kiberbezpetsi: metody zapobihannia ta zakhystu [Social engineering as a threat to cybersecurity: prevention and protection methods]. *Pedahohika bezpeky – Pedagogy of Security*, *9*(1), 37–42. https://doi.org/10.31649/2524-1079-2024-9-1-037-042 [in Ukrainian].