УДК 343.91:004(477) **DOI https://doi.org/10.32782/2522-9656/2026-19-2**

Афанасенко Світлана Іллівна,
кандидат юридичних наук, доцент, судовий експерт
відділу науково-методичного та інформаційно-
аналітичного забезпечення експертної діяльності
Одеського науково-дослідного інституту
судових експертиз
Міністерства юстиції України
ORCID ID: 0009-0008-3017-1683

ДОВІРА ТА ОБМАН У ЦИФРОВОМУ СЕРЕДОВИЩІ: РИЗИКИ ВІКТИМІЗАЦІЇ ТА ПРОФІЛАКТИЧНІ СТРАТЕГІЇ

TRUST AND DECEPTION IN THE DIGITAL ENVIRONMENT: RISKS OF VICTIMIZATION AND PREVENTIVE STRATEGIES

Анотація. У сучасному цифровому середовищі феномени довіри та обману набувають особливого значення, оскільки саме вони визначають рівень безпеки користувачів та їхню сприйнятливість до різноманітних форм маніпуляцій. Довіра виступає необхідною умовою функціонування соціальних мереж, електронної комерції, онлайн-освіти та державних електронних сервісів. Водночас вона стає вразливим місцем, яке активно використовують шахраї та маніпулятори для досягнення власних цілей. Обман у цифровому просторі проявляється у вигляді фішингу, соціальної інженерії, поширення дезінформації, маніпуляцій у соціальних мережах, а також у формі психологічного тиску, спрямованого на формування хибних переконань та прийняття невигідних рішень.

У статті розглянуто психологічні механізми довіри, що пояснюють схильність користувачів вірити навіть незнайомим джерелам інформації. Використання віктимологічного підходу дозволило виявити групи ризику та визначити чинники, які сприяють віктимізації у цифровому середовищі. Особливу увагу приділено аналізу правових аспектів протидії обману, зокрема міжнародним стандартам та національному законодавству у сфері кібербезпеки.

Запропоновано комплекс профілактичних стратегій, що включають правові інструменти, освітні програми з медіаграмотності, розвиток критичного мислення, а також технічні засоби захисту, такі як багатофакторна автентифікація та системи раннього виявлення шахрайських схем. Підкреслено необхідність міждисциплінарного підходу, який поєднує правові, психологічні та технологічні аспекти для ефективного захисту користувачів.

У висновках наголошується, що довіра є одночасно ресурсом і ризиком у цифровому середовищі, а обман – інструментом, який може призвести до серйозних наслідків для особи та суспільства. Розробка профілактичних стратегій має стати пріоритетом як для державних інституцій, так і для освітніх закладів та окремих користувачів.

Ключові слова: довіра, обман, цифрове середовище, віктимізація, профілактика, кібербезпека, медіаграмотність, соціальна інженерія.

Abstract. In the contemporary digital environment, the phenomena of trust and deception acquire particular importance, as they determine the level of user security and susceptibility to various forms of manipulation. Trust is an essential prerequisite for the functioning of social networks, e-commerce, online education, and public digital services. At the same time, trust becomes a vulnerable point actively exploited by fraudsters and manipulators to achieve their goals.

Deception in the digital sphere manifests itself through phishing, social engineering, disinformation, manipulations in social media, and psychological pressure aimed at shaping false beliefs and inducing disadvantageous decisions.

The article examines psychological mechanisms of trust that explain why users tend to believe even unfamiliar sources of information. A victimological approach makes it possible to identify risk groups and determine factors contributing to victimization in the digital environment. Special attention is paid to the analysis of legal aspects of counteracting deception, including international standards and national legislation in the field of cybersecurity.

A set of preventive strategies is proposed, combining legal instruments, educational programs on media literacy, the development of critical thinking, and technical protection tools such as multi-factor authentication and early fraud detection systems. The study emphasizes the necessity of an interdisciplinary approach that integrates legal, psychological, and technological dimensions to ensure effective user protection.

The conclusions highlight that trust is simultaneously a resource and a risk in the digital environment, while deception serves as a tool that may lead to serious consequences for individuals and society. Preventive strategies should become a priority for state institutions, educational establishments, and individual users.

Key words: trust, deception, digital environment, victimization, prevention, cybersecurity, media literacy, social engineering.

Постановка проблеми. Цифрове середовище стало ключовим простором соціальної взаємодії, де довіра виконує фундаментальну функцію – забезпечує сталість комунікацій, розвиток електронної комерції, освітніх платформ та державних сервісів. Водночас саме довіра перетворюється на чинник ризику, створюючи умови для маніпуляцій, шахрайства та віктимізації користувачів. Наукова проблема полягає у суперечності між потребою у довірі як основі цифрових комунікацій та її використанням як інструменту обману.

Теоретичні підходи демонструють подвійний характер довіри. Baier визначає її як необхідну умову соціальної взаємодії, що водночас робить індивіда вразливим [1 с. 231]. Rotter підкреслює, що довіра сприяє співпраці, але водночас створює ризик бути ошуканим [2 с. 5]. У цифровому середовищі ці ризики посилюються завдяки новим формам обману – від класичних шахрайських схем до технологій соціальної інженерії, що використовують штучний інтелект для створення переконливих, але хибних повідомлень [3, Article 324]. Луман трактує довіру як механізм зниження соціальної складності, проте визнає її потенціал для зловживань [4 с. 23]. Hardin наголошує, що довіра завжди пов'язана з ризиком і потребує інституційних гарантій [5 с. 78].

Емпіричні дослідження підтверджують цю суперечність. Gefen та співавтори доводять, що довіра є ключовим чинником розвитку електронної комерції, але водночас робить користувачів вразливими до шахрайських практик [6, с. 55]. Schmitt і Flechais показують, що генеративний штучний інтелект значно підвищує ефективність соціальної інженерії та фішингових атак [7, Article e0317232]. Попри наявність міжнародних стандартів і регуляцій, таких як рекомендації OECD щодо захисту споживачів [8, с. 12], стандарти цифрової

ідентифікації NIST [9, с. 15] та Digital Services Act ЄС [10, Art. 14], правові та технологічні інструменти залишаються недостатніми для повного захисту від маніпуляцій.

Отже, актуальність проблеми полягає у необхідності міждисциплінарного аналізу довіри та обману в цифровому середовищі, визначення їхнього впливу на ризики віктимізації та розробки профілактичних стратегій, що поєднують правові, психологічні та технологічні інструменти.

Мета статті полягає у комплексному дослідженні феноменів довіри та обману у цифровому середовищі, визначенні їхнього впливу на ризики віктимізації користувачів та розробці міждисциплінарних профілактичних стратегій, що поєднують правові, психологічні та технологічні інструменти.

Завдання дослідження передбачають: систематизацію наукових підходів до розуміння довіри та обману в цифровому просторі; аналіз психологічних механізмів довіри та їхньої ролі у формуванні сприйнятливості до маніпуляцій; окреслення основних форм цифрового шахрайства та соціальної інженерії; визначення чинників, що сприяють віктимізації користувачів; Дослідження міжнародного та національного досвіду правового регулювання у сфері кібербезпеки; розробку міждисциплінарних профілактичних стратегій, що інтегрують правові, психологічні та технологічні інструменти; формулювання практичних рекомендацій для державних інституцій, освітніх закладів та індивідуальних користувачів.

У класичних працях Baier довіра розглядається як необхідна умова соціальної взаємодії, але водночас як джерело вразливості [1, с. 231]. Rotter підкреслював її двоїстий характер: довіра забезпечує співпрацю, проте створює ризик бути ошуканим [2, с. 5]. Luhmann трактував довіру як механізм зниження соціальної складності, визнаючи її потенціал для зловживань [4 с. 23], а Hardin наголошував на необхідності інституційних гарантій, адже довіра завжди пов’язана з ризиком [5, с. 78].

У сучасних дослідженнях довіра у цифровому середовищі аналізується як ключовий чинник сприйнятливості користувачів до маніпуляцій та соціальної інженерії [3, Article 324]. Schmitt і Flechais довели, що генеративний штучний інтелект значно підвищує ефективність фішингових атак, створюючи повідомлення, які практично неможливо відрізнити від автентичних [7, Article e0317232]. Balakrishnan та співавтори показали, що найбільш уразливими є користувачі з низьким рівнем медіаграмотності, особи похилого віку та ті, хто мають обмежений досвід використання цифрових технологій [7, Article e0317232]. Водночас навіть високий рівень технічної компетентності не гарантує захисту, якщо відсутнє критичне мислення.

Правові інструменти у сфері кібербезпеки демонструють прагнення міжнародних інституцій врегулювати проблему маніпуляцій. Європейський Союз

у Digital Services Act намагається протидіяти дезінформації [10, Art. 14], а General Data Protection Regulation (GDPR) встановлює стандарти захисту персональних даних [11, Art. 5]. OECD у звіті *Protecting consumers in the digital age* наголошує на необхідності захисту споживачів [8 с. 12]. NIST у *Digital Identity Guidelines* рекомендує багатофакторну автентифікацію та інші інструменти для зниження ризиків шахрайства [9, с. 15]. Велика Британія у *Cyber Crime Strategy* розробляє освітні матеріали та створює центри для аналізу кіберзагроз [12, с. 45], а США реалізують програми протидії кібершахрайству через Міністерство юстиції та NIST [9, с. 40], [13, с. 50].

Попередні дослідження підтверджують, що ефективна профілактика можлива лише за умови міждисциплінарного підходу, який поєднує правові, психологічні та технологічні аспекти. Gefen та співавтори показали, що довіра є ключовим чинником розвитку електронної комерції, але водночас робить користувачів вразливими до шахрайських практик [6, с. 55].

Основні результати аналізу: довіра у цифровому середовищі має подвійний характер – вона є необхідною умовою комунікації, але водночас створює передумови для обману та віктимізації [1, с. 231], [4, с. 23], [5, с. 78]; основні форми обману включають фішинг, соціальну інженерію, дезінформацію та маніпуляції у соціальних мережах. Використання генеративного штучного інтелекту значно підвищує ефективність цих методів [3, Article 324], [7, Article e0317232]; групи ризику: найбільш уразливими є користувачі з низьким рівнем медіаграмотності, особи похилого віку та ті, хто мають обмежений досвід цифрових технологій [7, Article e0317232]; правові інструменти у сфері кібербезпеки потребують удосконалення, особливо щодо регулювання використання штучного інтелекту для шахрайських цілей [10, Art. 14], [11, Art. 25]; профілактичні стратегії мають бути комплексними: поєднувати правові, освітні та технічні заходи, включаючи багатофакторну автентифікацію, програми з медіаграмотності та розвиток критичного мислення [6, с. 55], [8, с. 30], [9, с. 40].

Отримані результати підтверджують, що довіра у цифровому середовищі є водночас ресурсом і ризиком. Вона забезпечує сталість комунікацій, але створює умови для маніпуляцій. Це узгоджується з класичними концепціями Baier [1, с. 231], Rotter [2, с. 5] та Luhmann [4, с. 23]. Правові механізми, такі як Digital Services Act та GDPR, демонструють прагнення врегулювати проблему, проте відстають від темпів технологічного розвитку. Тому міждисциплінарний підхід, що поєднує правові, психологічні та технологічні інструменти, є необхідною умовою ефективної профілактики.

Дослідження здійснено на основі міждисциплінарного підходу, що інтегрує правові, психологічні та технологічні аспекти аналізу феноменів довіри й обману у цифровому середовищі. Такий підхід дозволяє комплексно оцінити природу довіри, враховуючи не лише нормативно-правові рамки, але й

когнітивні механізми та технічні інструменти, які визначають рівень захищеності користувачів.

Для досягнення поставленої мети застосовано такі методи:

– Доктринальний аналіз правових норм та міжнародних актів у сфері кібербезпеки (Digital Services Act, GDPR) [10, Art. 14], [11, Art. 5].

– Контент-аналіз наукових публікацій, присвячених цифровому шахрайству, соціальній інженерії та використанню штучного інтелекту [3, Article 324], [7, Article e0317232].

– Психологічний аналіз механізмів довіри та когнітивних упереджень, що сприяють віктимізації користувачів [1, с. 231], [2, с. 5].

– Порівняльний метод**,** який дозволив зіставити український досвід із міжнародними практиками профілактики (OECD, NIST, ЄС) [8, с. 12], [9, с. 15], [10, Art. 22].

Застосування цих методів забезпечило комплексність дослідження, дозволило поєднати теоретичний аналіз із практичними аспектами кібербезпеки та сформувати основу для розробки міждисциплінарних профілактичних стратегій.

У ході дослідження встановлено: подвійний характер довіри у цифровому середовищі – вона є необхідною умовою комунікації, але водночас створює передумови для обману та віктимізації [1, с. 231], [4, с. 23], [5, с. 78]; основні форми обману включають фішинг, соціальну інженерію, дезінформацію та маніпуляції у соціальних мережах. Використання генеративного штучного інтелекту значно підвищує ефективність цих методів [3, Article 324], [7, Article e0317232].

Групи ризику: найбільш уразливими є користувачі з низьким рівнем медіаграмотності, особи похилого віку та ті, хто мають обмежений досвід використання цифрових технологій [2, с. 5]. Правові інструменти у сфері кібербезпеки потребують удосконалення, особливо щодо регулювання використання штучного інтелекту для шахрайських цілей [10, Art. 14], [11, Art. 25]. Профілактичні стратегії мають бути комплексними: поєднувати правові, освітні та технічні заходи, включаючи багатофакторну автентифікацію, програми з медіаграмотності та розвиток критичного мислення [6, с. 55], [8, с. 30], [9, с. 40].

Отримані результати підтверджують, що довіра у цифровому середовищі є одночасно ресурсом і ризиком. Вона забезпечує сталість комунікацій, але водночас створює умови для маніпуляцій. Це узгоджується з класичними концепціями Baier [1, с. 231], Rotter [2, с. 5] та Luhmann [4, с. 23].

Особливу увагу слід приділити правовому регулюванню: міжнародні акти, такі як Digital Services Act та GDPR, демонструють прагнення ЄС врегулювати питання дезінформації та захисту користувачів [10, Art. 14], [11, Art. 5]. Проте практика показує, що правові механізми відстають від технологічних

викликів, особливо у сфері використання штучного інтелекту для шахрайських схем [3, Article 324], [7, Article e0317232]. Це свідчить про необхідність постійного оновлення нормативної бази та її адаптації до швидких змін цифрового середовища.

Важливим є також психологічний аспект: навіть найсучасніші технічні засоби не гарантують захисту, якщо користувачі залишаються сприйнятливими до маніпуляцій. Когнітивні упередження, довірливість та відсутність критичного мислення створюють умови для віктимізації. Тому розвиток критичного мислення та медіаграмотності має стати ключовим елементом профілактики [2, с. 6; 6, с. 55].

Наукова новизна роботи полягає у міждисциплінарному аналізі довіри та обману у цифровому середовищі, що поєднує правові, психологічні та технологічні аспекти.

Запропоновано концепцію комплексних профілактичних стратегій, які включають: удосконалення правового регулювання у сфері кібербезпеки (Digital Services Act, GDPR) [10, Art.14], [11, Art.5]; освітні програми з медіаграмотності та розвиток критичного мислення [2 с. 6; 6, с. 55]; технічні засоби захисту, зокрема багатофакторну автентифікацію та системи раннього виявлення шахрайських схем (NIST, OECD) [8, с. 30; 9, с. 40].

Такий підхід дозволяє розглядати користувача не лише як пасивну жертву, але й як активного учасника цифрових взаємодій, здатного знижувати ризики віктимізації.

Довіра у цифровому середовищі має багатовимірний характер: вона формується на індивідуальному, інституційному та технологічному рівнях, і кожен із них може бути джерелом як стабільності, так і ризику. Ефективна профілактика потребує інтеграції правових норм із психологічними та освітніми заходами, адже навіть найсучасніші технічні інструменти не гарантують захисту без розвитку критичного мислення користувачів. Міжнародний досвід (ЄС, США, Велика Британія, OECD, NIST) підтверджує, що найбільш успішні стратегії базуються на поєднанні законодавчих ініціатив із практичною просвітницькою діяльністю.

Перспективні напрями дослідження: розробка моделей оцінки рівня довіри у цифрових комунікаціях та її впливу на ризики віктимізації; дослідження використання штучного інтелекту як інструменту обману та водночас як засобу захисту від шахрайства [3, Article 324], [7, Article e0317232]; порівняльний аналіз національних та міжнародних практик правового регулювання у сфері кібербезпеки [10, Art. 14], [11, Art. 5]; інтеграція профілактичних стратегій у систему освіти та професійної підготовки для формування стійкого цифрового суспільства [8 с. 30; 9 с. 40];Вивчення психологічних механізмів довіри у різних соціальних групах (молодь, особи похилого віку) з метою

розробки таргетованих програм профілактики; розробка інноваційних технічних рішень, що поєднують алгоритми штучного інтелекту із системами раннього попередження про шахрайські атаки.

У ході дослідження встановлено, що довіра у цифровому середовищі є водночас необхідною умовою комунікації та чинником ризику. Вона забезпечує сталість соціальних і економічних взаємодій, але створює передумови для маніпуляцій та шахрайства. Обман у цифровому просторі набуває нових форм – від класичних фішингових схем до використання генеративного штучного інтелекту для створення переконливих, але хибних повідомлень [3, Article 324], [7, Article e0317232].

Віктимізація користувачів зумовлена поєднанням психологічних механізмів довіри [1 с. 231; 2 с. 5], соціальних чинників та недосконалості правового регулювання [5 с. 78]. Це підтверджує подвійний характер довіри, який підкреслювали Baier, Rotter та Luhmann [1, с. 231; 2 с. 5; 4, с. 23].

Отримані результати свідчать про необхідність міждисциплінарного підходу до профілактики цифрового шахрайства, що має поєднувати: удосконалення правових норм та міжнародних стандартів кібербезпеки [10, Art. 14], [11, Art. 5]; розвиток критичного мислення та медіаграмотності користувачів [6, с. 55]; впровадження сучасних технічних інструментів захисту, включаючи багатофакторну автентифікацію та системи раннього виявлення шахрайських схем [8, с. 30; 9, с. 40].

Таким чином, довіра у цифровому середовищі має багатовимірний характер і може бути як ресурсом стабільності, так і джерелом ризику. Її ефективне управління потребує інтеграції правових, психологічних та технологічних стратегій, що забезпечить формування більш стійкого та безпечного цифрового суспільства.

Перелік використаних джерел:

1. Baier A. Довіра та антагонізм. *Ethics.* 1986. Т. 96, № 2. С. 231–260. DOI: 10.1086/292745.

2. Rotter J. Міжособистісна довіра, надійність та довірливість. *American Psychologist*. 1980. Т. 35, № 1. С. 1–7. DOI: 10.1037/0003-066X.35.1.1.

3. Schmitt M., Flechais I. Цифровий обман: генеративний штучний інтелект у соціальній інженерії та фішингу. *Artificial Intelligence Review*. 2024. Т. 57, Стаття 324. DOI: 10.1007/s10462-024-10973-2.

4. Luhmann N. Довіра та влада. Чичестер: Wiley, 1979. 146 с.

5. Hardin R. Довіра та надійність. Нью-Йорк: Russell Sage Foundation, 2002. 234 с. ISBN 9780871543483.

6. Gefen D., Karahanna E., Straub D. Довіра та TAM в онлайн-торгівлі: інтегрована модель. *MIS* Quarterly. 2003. Т. 27, № 1. С. 51–90. DOI: 10.2307/30036519.

7. Balakrishnan V., Ahhmed U., Basheer F. Особистісні, середовищні та поведінкові чинники, пов’язані з віктимізацією від онлайн-шахрайства серед дорослих. *PLOS One*. 2025. Т. 20, № 3. Стаття e0317232. DOI: 10.1371/journal.pone.0317232.

8. OECD. Захист споживачів у цифрову добу. OECD Digital Economy Papers. Париж: OECD Publishing, 2023. 54 с.

9. NIST. Керівні принципи цифрової ідентифікації. NIST Special Publication 800-63-4 (Draft). Гейтерсберг: National Institute of Standards and Technology, 2022. 76 с.

10. European Commission. Акт про цифрові послуги (Digital Services Act). Регламент (ЄС) 2022/2065. Брюссель: EU Publications, 2022. 112 с.

11. European Union. Загальний регламент про захист даних (GDPR). Регламент (ЄС) 2016/679. Брюссель: EU Publications, 2016. 88 с.

12. UK Home Office. Стратегія боротьби з кіберзлочинністю. Лондон: Home Office, 2020. 72 с.

13. U.S. Department of Justice. Боротьба з кібершахрайством. Вашингтон, D.C., 2021. 64 с.

14. Lee S., Kim H. Виявлення шахрайства на основі штучного інтелекту у Південній Кореї. *Journal of Cybersecurity*. 2023. Т. 9, № 2. С. 134–150.

15. INTERPOL. Глобальна стратегія боротьби з кіберзлочинністю. Ліон: INTERPOL Publications, 2023. 59 с.

References:

1. Baier, A. (1986). Trust and antitrust. *Ethics*, 96(2), 231–260. https://doi.org/10.1086/292745

2. Rotter, J. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist,* 35(1), 1–7. https://doi.org/10.1037/0003-066X.35.1.1

3. Schmitt, M., & Flechais, I. (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

4. Luhmann, N. (1979). *Trust and power.* Chichester: Wiley. 146 c.

5. Hardin, R. (2002). *Trust and trustworthiness*. New York: Russell Sage Foundation.

6. Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly,* 27(1), 51–90. https://doi.org/10.2307/30036519

7. Balakrishnan, V., Ahhmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. *PLOS One*, 20(3), Article e0317232. https://doi.org/10.1371/journal.pone.0317232

8. OECD. (2023). *Protecting consumers in the digital age.* Paris: OECD Publishing.

9. National Institute of Standards and Technology (NIST). (2022). *Digital identity guidelines (NIST SP 800-63-4 Draft)*. Gaithersburg: NIST. 76 c.

10. European Commission. (2022). *Digital Services Act (Regulation (EU) 2022/2065).* Brussels: EU Publications. 112 c.

11. European Union. (2016). *General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).* Brussels: EU Publications.

12. UK Home Office. (2020). *Cyber crime strategy*. London: Home Office. 72 c.

13. U.S. Department of Justice. (2021). *Combating cyber fraud*. Washington, D.C.: DOJ. 64 c.

14. Lee, S., & Kim, H. (2023). AI-based fraud detection in South Korea. *Journal of Cybersecurity*, 9(2), 134–150.

15. INTERPOL. (2023). *Global cybercrime strategy*. Lyon: INTERPOL Publications. 59 c.

Дата першого надходження статті до видання: 25.03.2026

Дата прийняття статті до друку після рецензування: 15.04.2026

Дата публікації (оприлюднення) статті: 19.05.2026