АКТУАЛЬНІ ПРОБЛЕМИ СУЧАСНОГО УКРАЇНСЬКОГО СУСПІЛЬСТВА

УДК 343.3/.7:004
DOI https://doi.org/10.32782/2707-9147.2024.102.3

А. В. ЗІНЮК
кандидат соціологічних наук,
доцент кафедри прикладної соціології та соціальних комунікацій
Харківський національний університет імені В. Н. Каразіна

М. І. НЕЧЕПОРЕНКО
магістрант кафедри прикладної соціології
та соціальних комунікацій
Харківський національний університет імені В. Н. Каразіна

ЦИФРОВА ЗЛОЧИННІСТЬ ЯК ПРОБЛЕМА ЦИФРОВОГО СУСПІЛЬСТВА

У статті зазначено, що цифрова злочинність є досить поширеною проблемою як для сучасного українського суспільства так і для всього світу. Цифрове середовище, частиною якого є майже кожен громадянин, має свої характерні особливості, наприклад анонімність та доступність. Відзначається, що дана проблема виникла в наслідок трансформації злочинності під впливом появи та розвитку цифрових технологій та швидко розповсюдилось й перетворилось на глобальну. Розповсюдженість цифрової злочинності, зокрема шахрайства в цифровому просторі, може створювати проблему для економіки, а деякі з проявів цифрової злочинності становлять загрозу національній безпеці, наприклад кібератаки чи втручання в роботу комп'ютерних систем критичної інфраструктури. Аналізуються поняття «аномія», «девіантність», а також розглядається класифікація видів цифрової злочинності. Автори зазначають, що одним з найбільш поширених видів цифрової злочинності, яка спрямована проти індивіда для отримання певної вигоди є фішинг – незаконний спосіб отримання конфіденційної інформації користувача (паролі, ім'я, банківські дані,) шляхом використання фейкових посилань, які часто замасковані під популярні ресурси або розповсюджується через спам повідомлення. Зріст цифрової злочинності може бути пояснений складним становищем в Україні, зокрема в економічній сфері – цей фактор, безумовно, впливає на рівень злочинності загалом, але цифрові злочини є більш «перспективними» з точки зору потенційного злочинця, адже вони є доступнішими, безпечнішими та вигіднішими. Робиться висновок, що про небезпечність цифрової злочинності свідчать

реакції урядів багатьох країн світу, які розробляють та адаптують законодавства для ефективнішої боротьби та запобігання цьому явищу.

Ключові слова: *цифрова злочинність, кіберзлочинність, злочинність, цифровізація, цифрове суспільство.*

Постановка проблеми. Епоха цифрової трансформації та досить швидких темпів цифровізації має як позитивні так і негативні наслідки, які мають безпосередній вплив на суспільство, його розвиток та процеси, які в ньому відбуваються. Цифровізація, з одного боку, дає можливість створювати ефективні засоби боротьби зі злочинністю, а з іншого – злочинці користуються тими перевагами, які надають цифрові технології. Таким чином, різні види злочинності адаптуються до навколишніх умов цифрового світу та трансформуються, в наслідок чого виникає нове явище – цифрова злочинність, боротьба з якою є значно складнішою через особливості цифрових технологій.

Сучасне суспільство перебуває в стані активної цифрової трансформації, в наслідок чого виникають нові можливості та виклики. Крім загальносвітових тенденцій, які впливають на поширення цифрової злочинності, українське суспільство перебуває в дуже важкому становищі, яке було викликане повномасштабною війною та іншими деструктивними процесами, що може створювати додаткові стимули для розвитку та поширення цифрової злочинності в Україні.

Тема злочинності була та є досить поширеною серед соціологів, але тема саме цифрової злочинності ще не була достатньо вивчена та висвітлена, що можна пояснити динамічністю даного явища, адже нові методи, мотивації та інші фактори трансформуються й видозмінюються так само швидко як і цифрове середовище.

Явище злочинності тісно пов’язана з явищем девіації та аномії Еміля Дюркгайма та Роберта Мертона. Ці явища є досить актуальними для сучасного українського суспільства, яке перебуває в стані постійних емоційних, соціальних, моральних, економічних та політичних потрясінь, що значною мірою загрожує виникненням аномічного стану суспільства.

Метою даної статті є розгляд цифрової злочинності як проблеми сучасності, її поширення та соціальних наслідків, які вона спричиняє.

Виклад основного матеріалу. Для цифрового суспільства характерне збільшення кількості слабких соціальних зв’язків, що, з одного боку, може стати причиною зменшення ступеню залучення індивіда (згідно теорії соціального контролю), а з іншого – ресурсом для засвоєння соціальних норм та цінностей (згідно теорії символічного інтеракціонізму). Завдяки сучасним цифровим технологіям ми маємо миттєвий доступ до інформації, а ця інформація, в свою чергу, тепер розповсюджується з великою швидкістю та не має тих обмежень, які були раніше, наприклад, географічних та лінгвістичних. Через це соціальні процеси відбуваються швидше і засвоєння нових суспільних правил потребує швидшої реакції від індивіда, інакше він ризикує залишитись в межах маргінальності чи девіації.

Види злочинності зазнали змін та адаптувались до нових умов, адже ті переваги, які пропонує цифровий простір значущі, наприклад анонімність, швидкість, мобільність, та доступність. За Стівеном Боксом, вищевказані фактори, а точніше їх сила, підвищують загрозу делікветної поведінки індивіда та знижують значущість соціального контролю [6].

«Цифровізація суспільства також сильно впливає на світ злочинності. Злочини трансформуються, наприклад, з точки зору типології та засобів. Злочинці змінюються, наприклад, їхні характеристики, їхні соціальні взаємодії і їхні стосунки з потенційними жертвами. Там, де є нові соціальні факти, нові звички, нові способи зустрічатися, купувати, платити, зберігати, захищати, передавати активи, нові цифрові ідентичності, нові системи для збору інформації, самоорганізації, задоволення та подорожей, цілком природно, що з'являються нові злочини та нові способи боротьби зі злочинністю» [7]. В наслідок трансформації злочинності в умовах цифрової інформаційної епохи виник новий тип злочинності – цифрова злочинність або кібер-злочинність.

«***Кіберзлочин*** *– суспільно небезпечне винне діяння в кіберпросторі та/ або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [2]. Тобто, з юридичної точки зору, кіберзлочинність класифікується як різновид звичайної злочинності.*

Розвиток цифрових технологій створює подвійний вплив на кіберзлочинність. З одного боку перехід, наприклад, банкінгу в цифровий простір створює нові можливості для злочинців, а з іншого – створюються механізми протидії та запобігання злочинним діям. Також з розвитком цифрових технологій з'являються нові види кіберзлочинів, які актуальні лише для цифрового простору. «Нові технології створюють нові можливості для злочинності. Завдяки глобалізації такі можливості зростають із «безпрецедентною швидкістю». Нові технології тепер стали суб'єктом (місцем), об'єктом (мішенню), знаряддям і символом злочину [8]».

Цифрова злочинність призводить до значних економічних збитків як окремих індивідів, бізнесу різного масштабу так і цілих країн. Це можуть бути будь-які прояви цифрової злочинності – від фішингу, шахрайства та крадіжки особистих даних, до кібер-атак та кібер-тероризму.

Цифрова злочинність здійснює значний вплив на приватність індивідів у сучасному цифровому соціумі. Кількість кібер-злочинів, яка постійно зростає створює серйозні загрози для особистої інформації та приватності користувачів. В залежності від типу цифрової злочинності вона має певний вплив на приватність:

Значні збитки приватній інформації користувачів Інтернету наносять кібер-атаки, ціллю яких є «зливи» інформації про користувачів. Такі крадіжки інформації можуть здійснюватися для продажу баз даних з інформацією про користувачів, для подальшого оприлюднення або для інших цілей. Такі «зливи» можуть бути різними за масштабами.

Таблиця 1

З якими видами цифрової злочинності стикались українці

Фішинг	21,9%
Вішинг (телефонне шахрайство)	71%
Віруси, трояни	46,2%
Кібер-шантаж	5,3%
Кібер-шпигунство	3,6%%
Хакінг	12,4%
Кібератака	8,3%
Кібертероризм	2,4%
Кібер-булінг	16%
Крадіжка особистої інформації	15,4%
Шахрайство під час онлайн покупок	37,3%
Шахрайство з банківськими картками	39,1%
З жодним з цих видів не стикався	10,1%

По данним авторського дослідження, проведеного у 2023 році, високим є рівень телефонного шахрайства (71%), шахрайства з банківськими картками (39,1%), шахрайства під час онлайн покупок (37,3%) та вірусів, троянів й іншого шкідливого програмного забезпечення (46,2%), але всього 10,1% респондентів не стикалися з переліченими видами цифрової злочинності.

Одним з найбільш поширених видів цифрової злочинності, яка спрямована проти окремого індивіда для отримання певної вигоди є фішинг – незаконний спосіб отримання конфіденційної інформації користувача (паролі, ім'я, банківські дані, тощо) шляхом використання фейкових посилань [4], які часто замасковані під популярні ресурси або розповсюджується через спам повідомлення. Цей тип виник завдяки поєднанню технічних можливостей цифрових технологій та соціальної інженерії та носить схожу назву – вішинг.

На сьогоднішній день в Україні набирають популярності шахрайські call-центри, які поєднують соціальну інженерію та цифрові технології для отримання незаконного прибутку. Точна кількість таких структур залишається невідомою завдяки перевагам анонімності, але про їхню розповсюдженість підтверджує стурбованість проблемою правоохоронних органів та згадки в масовій культурі. Тим часом за перші чотири місяці 2023 року було відкрито 26 734 таких справ – суттєво більше в порівнянні з минулими роками [1].

Такий різкий зріст цифрової злочинності може бути пояснений складним становищем в Україні, зокрема в економічній сфері – цей фактор, безумовно, впливає на рівень злочинності загалом, але

цифрові злочини є більш «перспективними» з точки зору потенційного злочинця, адже вони є доступнішими, безпечнішими та, в деякій мірі, вигіднішими. В таких умовах формуються злочинні угрупування, які, в свою чергу, погрожують суспільству значно сильніше, а ніж поодинокі злочинці. *«Організована кіберзлочинність може бути асоційована не тільки з проблемами інформаційної безпеки, але й із загрозами для державної безпеки, військово-промислового і виробничого комплексів, інфраструктури життєзабезпечення»* [3].

Цифрова злочинність може порушувати соціальну довіру в цифровому суспільстві на декількох рівнях. Зростання цифрової злочинності породжує сумніви в безпеці та приватності на онлайн-платформах та в соціальних мережах.

Загроза кібер-шахрайства підриває довіру до фінансових онлайн-транзакцій, люди можуть боятися здійснювати платежі в мережі через страх стати жертвою шахраїв. Це створює проблеми для онлайн-торгівлі та бізнесу, адже користувачі можуть стати менш активними в цифровому просторі та віддавати перевагу традиційній офлайн системі. Також подібні випадки шахрайства можуть впливати на довіру до державних інституцій – часто шахраї маскують свої фішингові (і подібні їм) оголошення під фінансову допомогу від держави. Саме через таку загрозу Міністерство соціальної політики України наголошує на тому, що необхідно довіряти лише перевіреним установам та не переходити на підозрілі/сторонні посилання [5].

Розповсюдження фейків та дезінформації кібер-злочинцями може підірвати довіру до цифрових медіа та інформаційних джерел. Люди можуть стати менш впевненими в правдивості інформації, яку вони знаходять в мережі, що підриває загальну довіру до цифрового простору та довіру між користувачами в ньому.

Цифрова злочинність має негативний вплив на довіру в суспільстві, оскільки вона порушує основні стовпи, які підтримують довіру і стабільність в цифровому середовищі. Цей вид злочинності може створювати загрозу для особистої безпеки та фінансового благополуччя людей, що призводить до відчуття нестабільності та небезпеки в інтернеті. Крім того, цифрова злочинність може підірвати довіру до електронних систем і послуг, таких як онлайн-банкінг, електронна ідентифікація та електронний уряд. Як було зазначено вище, цифрова злочинність впливає на довіру до медіа та інформаційних джерел. В світі, де дезінформація та фейки стають все більш поширеною проблемою, суспільство може ставити під сумнів достовірність інформації, яка знаходиться в цифровому середовищі.

Незважаючи на ті заходи, які проводять уряди багатьох країн світу, в тому числі й України, цифрова злочинність зберігає динаміку поширення та розповсюдження. Тому для подолання даної проблеми необхідні більш комплексні інституційні рішення, наприклад, підвищення цифрової грамотності населення. Отже, боротьба з цифровою

злочинністю і відновлення довіри в суспільстві – спільне завдання правоохоронних органів, експертів в цій сфері та суспільства в цілому. Належний захист та освіта в галузі цифрової безпеки є ключовими факторами в цьому процесі.

Також під час вивчення цифрової злочинності ми виявили, що цифрові злочини можливо категорізувати за багатьма ознаками, наприклад за мотивацією злочинців, інструментами, які вони використовують, тощо. Так, приміром, існують злочини метою яких є фінансове збагачення – більшість видів, які пов'язані з шахрайством. Також можливо розділяти злочини за складністю їх реалізації – для деяких видів цифрових злочинів необхідне технічне забезпечення та навчання, тоді як інші цього не вимагають.

Сучасні проблеми цифрового суспільства, особливо такі складні та малодосліджені, вимагають від нас адаптації та пошуку нових шляхів і методів їх вивчення. Цифрова злочинність створює серйозні виклики для суспільства, яке перебуває в процесі цифрової трансформації, а особливо для українського суспільства, яке перебуває в стані перманентних потрясінь. Дане явище створює перешкоди для економіки, соціальної довіри та навіть може викликати міжнародні скандали, які можуть погіршити й без того складні умови сьогодення. Тому дана проблема вимагає особливої уваги та вивчення не тільки криміналістами чи правоохоронними органами, але й іншими дослідниками, зокрема й соціологами.

Список використаної літератури

1. Богданьок О. В Україні зафіксували рекордну активність шахраїв. *Суспільне. Новини.* Режим доступу: URL: https://suspilne.media/494884-v-ukraini-zafiksuvali-rekordnu-aktivnist-sahraiv-opendatabot/

2. Вадовський В. Кіберзлочинність в Україні. *EQUITY.* Режим доступу: URL: https://equity.law/press-center/publications/1169.html

3. Гребенюк М., Черняк А. Проблеми протидії організованої злочинності у сфері цифрової економіки. *Підприємництво, господарство і право*. 2019. № 3. С. 297–302. Режим доступу: URL: http://pgp-journal.kiev.ua/archive/2019/3/57.pdf

4. Думчиков С., Лукічов В. Статистика фішингових інцидентів в Україні за 2021 рік. Електронний ресурс. Режим доступу: URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34523/91970.pdf?sequence=2&isAllowed=y

5. Міністерство соціальної політики України. Міністерство соціальної політики України. Режим доступу: URL: https://www.msp.gov.ua/news/22517.html

6. German L. Online identity. COMP6044. 2010. URL: https://blog.soton.ac.uk/comp6044/category/discipline/criminology-discipline/page/2/

7. Global cybercrime costs $600 billion annually – study. RAPPLER. 2018. URL: https://www.rappler.com/technology/196606-global-cybercrime-costs-mcafee-csis-study/

8. Nuth M. N. Taking advantage of new technologies: For and against crime. Norwegian research center for computers and law (NRCCL), University of Oslo, Norway 2008. URL: https://www.sciencedirect.com/science/article/abs/pii/S026736490800099X

Zinyuk A. V., Necheporenko M. I. Digital crime as a problem of digital society

The article states that digital crime is a fairly widespread problem both for modern Ukrainian society and for the whole world. The digital environment, of which almost every citizen is a part, has its own characteristics, such as anonymity and accessibility. It is noted that this problem arose as a result of the transformation of crime under the influence of the emergence and development of digital technologies and quickly spread and turned into a global one. The prevalence of digital crime, in particular fraud in the digital space, can pose a problem for the economy, and some of the manifestations of digital crime pose a threat to national security, such as cyber attacks or interference with the operation of critical infrastructure computer systems. The concepts of "anomy", "deviance" are analyzed, and the classification of types of digital crime is considered. The authors note that one of the most common types of digital crime, which is directed against an individual in order to obtain a certain benefit, is phishing – an illegal way of obtaining confidential user information (passwords, name, bank data) by using fake links, which are often disguised as popular resources or distributed through spam messages. The growth of digital crime can be explained by the difficult situation in Ukraine, in particular in the economic sphere – this factor certainly affects the level of crime in general, but digital crimes are more "promising" from the point of view of a potential criminal, because they are more accessible, safer and more profitable. It is concluded that the danger of digital crime is evidenced by the reactions of the governments of many countries around the world, which are developing and adapting legislation to more effectively combat and prevent this phenomenon.

Key words: *digital crime, cybercrime, crime, digitalization, digital society.*