Ковальчук А.Ю.,
доктор юридичних наук, професор,
професор кафедри міжнародного
права та галузевих правових
дисциплін,
Київський університет права НАН
України
(м. Київ, Україна)

КІБЕРЗЛОЧИННІСТЬ 2025: ЗАЛУЧЕННЯ ВРАЗЛИВИХ ГРУП ЯК СТРАТЕГІЯ УНИКНЕННЯ ПОКАРАННЯ

В Україні кількість кримінальних правопорушень, які відносять до категорії кіберзлочинів, постійно збільшується і набуває нових форм реалізації. Це наслідки сучасної синергії державних і недержавних акторів у ведені гібридних конфліктів, яка посилює виклики для глобальної безпеки. Нині кіберзлочинність функціонує як бізнес, який розширюється за рахунок нових учасників та нових способів проникнення у «критичне» середовище. Відповідно, діють закони ринку: попит породжує пропозицію надання послуг з забезпечення ефективності у реалізації кібератаки. Як і в будь-якому іншому бізнесі, економія на масштабі допомагає заробляти більше грошей, й вчиняти більш витончені й непомітні атаки, але наслідки їх подекуди катастрофічні. Такий тренд висвітлюється й у статистиці. Вивчаючи ландшафт злочинності і якісний склад злочинних груп було виявлено наступні зміни – зростання показників залучення неповнолітніх до вчинення кіберзлочинів, а також вчинення кіберзлочинів жінками (за 3 місяці 2025 року виявлено 35 жінок (41,7 %), які вчинили кримінальні правопорушення, передбачені статтями Розділу XVI КК України). Кількість злочинів вчинених неповнолітніми: у 2025 році обліковано 9 кримінальних правопорушень вчинених неповнолітніми або за їх участю, у 2024 році – 5. Варто звернути увагу на статистичні дані про виявлених осіб, які вчинили кримінальні правопорушення у минулих роках. До речі, таких осіб виявлено 259, що у 3,1 раза більше порівняно з тими, що вчинили кримінальні правопорушення за 3 місяці 2025 року. Кожна третя особа – жінки – 94 (36,3 %).

За 2024-2025 роки виявлено 84 особи, які вчинили кримінальні правопорушення у групі, в т.ч. 48 – у складі організованої групи або злочинної організації, з них 7 – з корупційними зв'язками. У складі групи – за участю неповнолітніх (змішаної групи) – 12 осіб, тільки неповнолітніми – 3[1].

Також виявлено, що у цифровому просторі ролі учасників кіберзлочинних груп розподілені за іншою схемою, це у першу чергу пов'язано з їх транскордонністю. Діти, жінки здебільшого залучаються як виконавці, або вербувальники. Чим легше потенційному зловмиснику здійснити атаку, тим більша ймовірність, що він спробує. На таку закономірність легко залучають дітей. Жінки, як новий тренд, залучаються завдяки ірраціональному способу мислення, та обрання не тривіальних

підходів до вчинення злочинних дій, саме така якість жінок становить інтерес у організаторів кібератак. А ще жінки дисциплінованіше і більш відповідальні та дуже обережні, що у сукупності своїх якостей робить їх вразливими/сильними на «ринку» кіберзлочинності.

Окремо слід відмітити, що кіберзлочинні групи спеціалізуються не лише на кібератаках на державні об'єкти, а й приймають участь й у інших видах злочинів які потенційно можуть бути пов'язані з більш резонансними атаками, а також з фінансуванням тероризму. Маючи спеціальні технічні навички та вміння, міжнародні організовані злочинні угруповання можуть використовувати віртуальні валюти для фінансування терористичних заходів, вербування нових учасників, здійснення терористичних актів тощо. Хоча на сьогодні виявлено мало злочинних мереж які спеціалізуються суто на криптовалютах, можна припустити, що це пов'язано з залученнями агентів штучного інтелекту. Наприклад, кейс «The Terminal of Truth» (Термінал істин-ToT) продемонстрував, як агент штучного інтелекту (ШІ) автономно брав участь в екосистемі криптовалюти, накопичуючи багатство в цифрових активах через взаємодію з людьми та агентами-ботами ШІ. Це підкреслює потенціал агентів штучного інтелекту для взаємодії з цифровою економікою таким чином, щоб сприяти постійному масштабному шахрайству[2]. У той же сфері дітей, жінок ефективно залучають у якості трейдерів, міксерів та обмінників.

Дослідження проблеми залучення жінок і дітей до злочинних мереж у кіберпросторі показав проблему «сучасного рабства». Деяких змушують ставати співучасниками злочинів, пов'язаних з торгівлею людьми [3]. Дефіцит засобів до існування, роз'єднання сімей, погіршення психічного благополуччя створюють нові умови для криміналізації добропорядних громадян. Так, сінгапурська практика протидії серйозній та організованій злочинності показує залучення вразливих категорій осіб у якості «грошового мула» (Money mules), які сприяють переміщенню грошей здобутих злочинним шляхом. Грошові мули – це зазвичай особи, які передають контроль над своїми платіжними рахунками, наприклад, банківськими й соціальними, злочинцям, або які використовують свої платіжні рахунки для отримання чи переказу грошей за вказівками злочинців [4]. В Україні такий вид фінансової експлуатації не зареєстрований хоча не виключно що існує.

Слід зазначити, що у деяких країнах гендерні ролі роблять жінок менш підозрюваними в кіберзлочинах тому на них менше звертають увагу правоохоронні органи. Жінку ж штовхають на такі дії різні мотивації. Так, у патріархальних культурах гендерна дискримінація може сприяти тому, що жінки намагаються довести свою компетентність через нелегальні дії в онлайн-середовищі. Такі зміни необхідно вивчати й досліджувати у контексті побудови політики безпеки.

Загальний аналіз тенденцій кіберзлочинності в Україні свідчить про її швидку трансформацію, омолодження складу учасників і активне залучення жінок, що відображає глобальні виклики безпеці. Кіберзлочинність перестала бути прерогативою технічних фахівців-чоловіків і дедалі більше включає

вразливі категорії — дітей, жінок, а також осіб з обмеженими ресурсами. Це відбувається на тлі зростання попиту на кримінальні послуги у цифровому середовищі, яке сприяє формуванню тіньової економіки в кіберпросторі. Участь жінок і неповнолітніх у таких злочинах пояснюється як психологічними й соціальними факторами, так і стратегічним розрахунком з боку організованих груп. Жінки сприймаються як менш помітні для правоохоронних органів, а діти — як інструмент уникнення кримінальної відповідальності. Також відзначається нове явище — використання жінок і дітей у злочинних криптоекономічних схемах, що межують з явищами сучасного рабства. Важливим є й те, що кіберзлочинність часто поєднується з іншими формами організованої злочинності: фінансуванням тероризму, торгівлею людьми, корупцією, що вказує на зростаючий рівень складності кіберзагроз.

***Список використаних джерел*:**

1. Офіс Генерального прокурора України: Єдиний звіт про кримінальні правопорушення (Форма 1), Єдиний звіт про осіб, які вчинили кримінальні правопорушення (Форма 2). URL: https://gp.gov.ua/ua/posts/statistika
2. Terminal of Truths: Guide to the Future of AI (2024). URL: https://airdropalert.com/blogs/terminal-of-truths-guide/
3. Національні механізми взаємодії об'єднання зусиль для захисту прав осіб, які постраждали від торгівлі людьми. Практичний довідник: друге видання (2022).URL: https://www.osce.org/files/f/documents/9/a/548020.pdf
4. Amendments to the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act and the Computer Misuse Act. URL: https://www.mha.gov.sg/mediaroom/press-releases/amendments-to-the-corruption-drug-trafficking-and-other-serious-crimes-confiscation-of-benefits-act-and-the-computer-misuse-act/
5. Top 10 Best-Known Cybersecurity Incidents and What to Learn from Them (2024). URL: https://www.ekransystem.com/en/blog/top-10-cyber-security-breaches
6. Understanding and Conceptualizing Domestic Terrorism: Issues for Congress (2023). URL: https://www.everycrsreport.com/reports/R47885.html