СУЧАСНІ ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ПРОБЛЕМИ КРИМІНОЛОГІЇ

УДК 343.91/.97:004.056(477) *DOI: https://doi.org/10.32631/vca.2025.2.5*

Петро Петрович ГАЛУШКО
(Харківський національний університет внутрішніх справ, м. Харків)

ОСОБА КІБЕРЗЛОЧИНЦЯ: КРИМІНОЛОГО-ТИПОЛОГІЧНА ХАРАКТЕРИСТИКА

У статті досліджено кримінологічні підходи до типології кіберзлочинців у контексті стрімкої ескалації загроз у цифровому середовищі. Акцентується увага на потребі переосмислення традиційних положень кримінологічної теорії в умовах постіндустріального розвитку суспільства, зокрема через ускладнення структури кіберзлочинності та зростання її впливу на соціальні відносини. Підкреслюється значення глибокого аналізу особистості злочинця як ключового елементу для розробки ефективних заходів запобігання. Обґрунтовано необхідність формування типології кіберзлочинців, яка дозволяє виділяти спільні риси, мотиви й поведінкові моделі осіб, що вчиняють кримінальні правопорушення у кіберпросторі. Наводиться огляд наукових підходів до проблеми, аналізуються труднощі виокремлення типових профілів кримінальних правопорушників у зв'язку зі специфікою кіберзлочинності. Особлива увага приділена дослідженню особистісних, психофізіологічних та соціальних характеристик осіб кіберзлочинців.

Ключові слова: *кіберзлочинність, кримінологічна типологія, особа кримінального правопорушника, комп'ютерні злочини, цифрове середовище, кримінально протиправна поведінка, психологічні характеристики, протидія кіберзлочинності.*

Постановка проблеми. У контексті зростання масштабів кіберзлочинності, ускладнення її структури та трансформації злочинної поведінки у цифрову площину, зростає потреба в оновленні кримінологічних підходів до вивчення особи злочинця. Постіндустріальна стадія розвитку суспільства висуває нові виклики перед наукою кримінології, що зумовлює формування нової теоретичної парадигми. Особливого значення набуває проблема кримінологічної типології кіберзлочинців, як засобу систематизації знань про злочинну поведінку в цифровому середовищі.

Питання дослідження особистості злочинця в кримінології мають

глибоке теоретичне підґрунтя. Вагомий внесок у розробку цієї проблематики зробили такі вчені, як О. М. Костенко, С. Ф. Денисов, К. О. Лагода, Ю. В. Орлов, І. М. Даньшин, які досліджували як загальні питання особи правопорушника, так і специфіку кримінологічного аналізу в умовах новітніх форм злочинності. Зокрема, питання кіберзлочинності та типології її суб'єктів розглядали М. О. Кравцова, Р. В. Бараненко, В. В. Топчій, Л. В. Борисова, Д. С. Азаров, які підкреслювали ускладненість характеристик особи кіберзлочинця та недостатню розробленість єдиної типологічної моделі.

Таким чином, актуальність дослідження зумовлена необхідністю розроблення кримінологічно обґрунтованої типології осіб, що вчиняють правопорушення у сфері інформаційних технологій, для ефективнішої протидії новітнім формам злочинної поведінки.

Мета статті полягає у здійснення кримінологічної типології кіберзлочинців.

Виклад основного матеріалу. Ескалація загрози кіберзлочинності та її значний вплив на окремих осіб, організації та держави є дедалі очевиднішою. Зростаючий обсяг і складність кібератак зумовлюють необхідність глибшого розуміння осіб, які їх вчиняють. Постіндустріальна стадія розвитку людства вимагає переосмислення й уточнення багатьох положень кримінологічної теорії, перегляду традиційних підходів до боротьби зі злочинністю. На сучасному етапі кримінологія проходить етап формування нової парадигми, зміни наукового світогляду, генерування ідей та упровадження інновацій[1]. Отже, кримінологічне дослідження особистості злочинця має виключне значення для забезпечення повноти пізнання феномену злочинності та, відповідно, розробки заходів запобігання. Кримінологічна типологія – це система класифікації, яка використовується для розуміння злочинної поведінки. Вона допомагає вивчати, як і чому відбуваються злочини, шляхом об'єднання злочинців у групи на основі спільних рис, мотивів або способів вчинення злочинів.

Типологія кіберзлочинців дасть можливість хоча б умовно поділити їх на види, виокремити їхні особливості. Така інформація дозволить скласти більш точні профілі осіб, які вчиняють злочини з використанням мережі Інтернет, розробити рекомендації для звичайних громадян, які можуть стати жертвами кіберзлочинців[2].

У кримінології особа, яка вчинила кримінальне правопорушення, досліджується найбільш ґрунтовно, усебічно, адже вона є одним з основних елементів предмета, перебуває на межі низки правових наук, а також соціології, психології, педагогіки, що, у свою чергу обумовлює використання методів для предметного вивчення особи злочинця та типології кіберзлочинця.

[1] Головкін Б. М. Теперішнє і майбутнє кримінології. *Проблеми законності*. 2020. № 149. С. 169.

[2] Чередниченко К. Ю. Кримінологічна типологія кіберзлочинців // Злочинці і жертви злочинів : матеріали XX всеукр. наук. конф. з кримінології для студентів, аспірантів та молодих вчених, м. Харків, 16 листоп. 2020 р. Харків, 2020. С. 711–716.

О. М. Костенко розвіває ідею, що під методом кримінологічного дослідження слід розуміти узгоджену з принципом кримінологічного пізнання сукупність прийомів, що застосовуються для пізнання злочинності, її причин і умов, особистості злочинця і розробки заходів протидії злочинності[1]. Крім того, саме досліджуючи особистість злочинця, можна визначити ті Кримінологічно значущі характеристики середовища, які іноді важко (або неможливо) виявити іншим шляхом[2].

Складність досліджуваного питання обумовлює тим, що не було б сенсу вести мову про особистість злочинця, якщо їй не притаманні властивості, відмінні від особистісних якостей тих, хто не вчиняє злочинів. Для кримінолога особистість становить інтерес не сама по собі, а лише тією мірою, якою її властивості детермінують злочинну поведінку. Як підкреслюють К. О. Лагода та Ю. В. Орлов, кримінологія, вивчаючи особистість злочинця у нерозривному зв'язку з антисуспільною поведінкою, не може не спиратися в теоретичних концепціях та практичних висновках саме на особливості якостей осіб, які вчиняють злочини[3]. та становить об'єкт запобіжного впливу на індивідуальному та спеціально-кримінологічному (щодо групи осіб з типовими антисуспільними рисами) рівнях. Отже визначити та впровадити ці відносини з кримінологічної точки зору можливо лише тільки через дослідження конкретних особистостей та їхні взаємостосунки з іншими суб'єктами. Власне ці відносини, що складаються в напряму вчинення злочину, ведення антисоціального способу життя, що притаманне правопорушникам, і формують відповідний тип особи, яка в кримінології називається особа злочинця[4].

Згідно з позицією І. М. Даньшина, про особу злочинця можна говорити у зв'язку з настанням юридично значущої події – вчиненням діяння, передбаченого законом про кримінальну відповідальність. Інакше і бути не може, оскільки властивості та якості будь-якої людини, у тому числі й злочинця, знаходять свій вияв не інакше, як в її діях і діяльності, а також у домінуючих орієнтаціях і мотиваціях. Але ця думка, на наш погляд, застаріла та в свою чергу можемо погодитися з точкою зору А. Ф. Зелінського О М. Литвинова та Ю. В. Орлова та наголосити що такий підхід є занадто формальним і не враховує мінливості сучасної злочинності, яка багато в чому залежить від зміни законодавства про кримінальну відповідальність і роботи органів кримінальної юстиції. Так, Ю. В. Орлов вказав, що особистість кримінального правопорушника – відкрита, динамічна, соціально-біологічна система якостей людини, винної у злочинній діяльності як систематичній кримінальній практиці чи одиничному

[1] Костенко О. М., Перелигіна Р. В. Методологія і доктрина сучасної кримінології. К. : КУП НАН України, 2016. С. 6

[2] Кваша О. О. Організатор злочину кримінально-правове та кримінологічне дослідження. К. : Ін-т держави і права ім. В. М. Корецького, 2003. С 121.

[3] Лагода К. О., Орлов Ю. В. Невиконання судового рішення: кримінологічна характеристика та запобігіння : монографія / за заг. ред. О. М. Литвинова. Харків : ТОВ «В деле», 2016. С. 48

[4] Кримінологія : підручник / А. М. Бабенко, О. Ю. Бусол, О. М. Костенко та ін.; за заг. ред. Ю. В. Нікітіна, С. Ф. Денисова. Є. Л. Стрельцова. 2-ге вид., перероб. і допов. Харків : Право, 2018. С. 128–129.

особистісно значущому кримінальному досвіді. Вона не зводиться виключно до соціально значущих рис людини[1].

Таким чином, сьогодні в кримінологічній літературі розглядаються різні думки стосовно сутності змісту самого поняття особа злочинця. В зв'язку з цим С. Ф. Денисов справедливо вказує, що особа злочинця є достатньо складним феноменом, інтегруючим і багатовекторним поняттям[2], а тому потребує більш грунтовного системного асиметричного аналізу.

Для кращого розуміння злочинної поведінки кримінологи використовують класифікаційні схеми, відомі як типології злочинів, для вивчення того, як і чому відбуваються девіантні дії під час вчинення злочину. Центральним і важливим міркуванням будь-якої типології є її актуальність для суспільства. Кримінолог, який вивчає типологію злочинів, повинен визнати, що злочини минулого не обов'язково збігаються зі злочинами, скоєними сьогодні.[3] У контексті кіберзлочинців кримінологічна типологія передбачає класифікацію злочинців на різні категорії на основі спільних характеристик для кращого розуміння їхньої поведінки. Ця структура допомагає вивчати «як» і «чому» були вчинені кіберзлочини, особливо під час війни росії проти України.

Кримінологічні дослідження особи комп'ютерного злочинця базуються в основному на двох особливо значимих специфічних групах відомостей. По-перше, це відомості про особу невідомого комп'ютерного злочинця. Такі відомості будуються в основному на основі залишених комп'ютерним злочинцем матеріальних слідах як на місці події комп'ютерного злочину, так і ідеальних слідах відображених в пам'яті свідків, потерпілих тощо. Очевидно, що такі відомості дозволяють сформулювати уяву про загальні риси, ознаки та манери поведінки комп'ютерного злочинця. По-друге, це відомості, які характеризують риси, ознаки та манери поведінки для встановлення відомого комп'ютерного злочинця[4].

Як зазначила Л. В. Борисова «сьогодні кіберзлочинцям вченими надаються неоднозначні соціально-психологічні характеристики, які засновані на узагальнених емпіричних даних, оскільки сам предмет розгляду недостатньо вивчений з причин специфічності й складності цих злочинів»[5]. В свою чергу Д. С. Азаров, наголосив: «На жаль, вітчизняна кримінологія не має у своєму арсеналі даних узагальнюючого характеру

---

[1] Кримінологія (Загальна частина) : навч. посіб. / [І. О. Бандурка, О. М. Литвинов, Ю. В. Орлов та ін.] ; за заг. ред. д-ра юрид. наук, проф. Ю. В. Орлова ; МВС України, Харків. нац. ун-т внутр. Справ Харків : ХНУВС, 2025. С. 231.

[2] Денисов С.Ф. Особа злочинця у кримінологічній теорії України. Вісник Кримінологічної асоціації України. 2020. № 1 (22). С. 152–159.

[3] Introduction to Criminal Justice / Wesley B. Maier, Kadence C. Maier, William M., Terry D. Edwards. URL: https://openwa.pressbooks.pub/crimjust1/

[4] Малій М. І. Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження : дис. ... канд. юрид. наук : 12.00.08. Хмельницький, 2021. 213 с.

[5] Борисова Л. В. Суб'єкт (особа) транснаціонального комп'ютерного злочину : криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права*. 2008. Вип. 44. С. 76–80.

щодо особи цих злочинців, майже відсутні публікації з цього приводу. А окремі характеристики «комп'ютерного злочинця» (як то: вік – 24–25 років (середній вік – 30 років); за освітою – інженер в галузі електроніки і математики, займає відповідальну посаду (віце-президент компанії, фінансові керівники, скарбники, вкладники капіталів тощо); можуть не мати ніякої технічної освіти; не мають кримінального минулого; більшість становлять чоловіки, але можуть зустрічатися й жінки; у цілому це яскрава, думаюча, творча особа, професіонал своєї справи, готовий прийняти технічний виклик, бажаний працівник»[1].

Треба сказати, що з визначенням типології кіберзлочинців, на жаль, складно. Немає єдиного підходу та розуміння такого поняття. Так, В. В. Топчій вказав, що «у міжнародних нормативно-правових актах універсальне коло кримінальних правопорушень у сфері інформаційних відносин досі не визначене. Це пов'язано з динамічним розвитком злочинності, виникненням нових видів кримінальних правопорушень, що вчиняються у сфері інформаційних технологій. Тому на сьогодні актуальним питанням залишається розроблення єдиної кримінальної стратегії, пов'язаної з комп'ютерними кримінальними правопорушеннями, їх поняттям і системою»[2]. Такої ж думки Т. Д. Лисько, В. В. Меланіч та Ю. В. Славіта: «Окрім змін у кримінальному законодавстві, комплексна боротьба з кіберзлочинністю потребує гармонізації національного кримінального законодавства про кіберзлочинність із міжнародним, що позитивно вплине на стан боротьби та запобігання кіберзлочинності»[3].

На нашу думку, кримінологічна типологія є засобом розробки загальних підсумкових тверджень щодо спостережуваних фактів про певний клас (тип) злочинців, які є достатньо однорідними, щоб їх можна було розглядати як тип, а не намагатися вивчати злочинців як єдиний вид. Це систематичне групування сутностей, які мають спільні характеристики або ознаки, до класів певної системи. Типології є важливим інструментом у кримінології, що допомагає науковцям, правоохоронним органам зрозуміти різні види злочинів, кримінальних правопорушень і злочинної поведінки. Класифікація злочинів є необхідною, оскільки не всі злочини однакові. Кримінологи використовують типології злочинів, щоб вивчати, чому відбуваються злочини, хто їх вчиняє та як їх можна запобігти[4].

Відомо, що перше в Україні дослідження портрета комп'ютерного злочинця здійснене ще у 1997 році[5]. Дану працю побудовано на основі

---

[1] Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. … канд. юрид. наук : 12.00.08 / НАН України ; Інститут держави і права ім. В. М. Корецького. К., 2002. С. 135.

[2] Топчій В. В., Бодунова О. М. Система кримінальних правопорушень у сфері інформаційних технологій: міжнародно-правовий вимір. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 1 (10). С. 187–194.

[3] Лисько Т. Д., Меланіч В. В., Славіта Ю. В. Протидія кіберзлочинності: сучасний стан вітчизняного законодавства та досвід зарубіжних країн. *Актуальні проблеми держави і права*. 2022. № 96. С. 44–49. DOI: https:// doi.org/10.32782/apdp.v96.2022.4.

[4] Docs criminal justice glossary. Crime typologies. URL: https://docmckee.com/cj/docs-criminal-justice-glossary/crime-typologies-definition.

[5] Малій М. І. Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження : дис. ... канд.

узагальнення вітчизняного та зарубіжного досвіду дослідження характерних рис і ознак особи комп'ютерного злочинця. Крім того в даному дослідженні розкривається сутність поняття особи комп'ютерного злочинця, розкрита характеристика особи комп'ютерного злочинця та сформульована класифікація комп'ютерних злочинців, які вчиняли злочини 25-30 років тому. Водночас, судова-слідча статистика та практика свідчить про стрімке зростання кількості вчинених комп'ютерних кримінальних правопорушень в світі за останні роки. Виходячи з даних позицій, вважаємо, що комп'ютерні злочинці, які вчиняють комп'ютерні злочини сьогодні у Всесвітній мережі інтернет потребують спеціального і більш детального наукового дослідження. Особливо нагальними питаннями при дослідженні особи комп'ютерного злочинця є вивчення його особистісних якостей, психофізіологічних особливостей, індивідуальних рис та ознак, притаманних саме йому та закономірностей його поведінки при вчиненні комп'ютерних злочинів. Для цього потрібно більш детально розглянути зарубіжний досвід та досвід зарубіжних науковців.

Як ми вже казали вище, не існує єдиного міжнародно узгодженого визначення кіберзлочинності. Загалом, це будь-яка незаконна діяльність, що відбувається в кіберпросторі, з використанням мережі та призводить до матеріальних збитків; або незаконне використання будь-якого комунікаційного пристрою для вчинення незаконного діяння. Альтернативні терміни включають «злочин у кіберпросторі», «комп'ютерний злочин», «електронний злочин», «високотехнологічний злочин» і «злочин із використанням технологій». Кіберзлочинність часто передбачає використання комп'ютера як інструмента або цілі. Важливим є розрізнення між кіберзалежними та кібернетично сприяючими злочинами. Не будемо сперечатися з Дж. С. Албанезе, який сказав, що кіберзалежні злочини не можуть існувати поза цифровим світом, тоді як кібернетично-сприяючі злочини є традиційними злочинами, яким сприяють технології. Існуючі внутрішні типології виділяють в структурі кіберзлочинності такі її прояви, як кіберпроникнення, кібершахрайство та крадіжки, кіберпорнографію, а також кібернасильство.[1] Це вказано і в Конвенції Ради Європи про кіберзлочинність від 23.11.2001 р.[2]

Проаналізувавши позиції, поширені серед зарубіжних кримінологів, можна дійти висновку про те, що у них інший підхід до типології та ознак осіб, які вчиняють каберзлочини. Вони виділяють основні 4 групи за критеріями мотивації, особливостей технічних навичок та досвіду, цілепокладання, організаційної структури й характеру взаємодії з іншими співучасниками.

Домінуючі мотиви, що спонукають кіберзлочинців до їх протиправної

юрид. наук : 12.00.08. Хмельницький, 2021. С. 112.

[1] Albanese Jay S. A Typology of Cybercrime: An Assessment of Federal Prosecutions. *Journal of Criminal Justice and Law*. 2022. Vol. 6. Issue 1. URL: https://jcjl.pubpub.org/pub/vm45gchn/release/1.

[2] Конвенція про кіберзлочинність : Міжнародний документ Ради Європи. Конвенція від 23.11.2001 р. URL: : https://zakon.rada.gov.ua/laws/show/994_575#Text.

активності, є різноманітними та складними. Розуміння мотивації має вирішальне значення для розробки ефективних стратегій протидії кіберзлочинностц. Можна виділити такі ключові мотиви:

● ***корисливий мотив, спрямований на отримання фінансової вигоди:*** це є головним рушієм для багатьох кіберзлочинців, охоплюючи такі дії, як незаконне заволодіння персональними даними, їх продаж, а також шахрайства, атаки програм-вимагачів тощо[1]. Чорний ринок викрадених даних і легкість їх монетизації сприяють цій активній дії цього мотиву. Модель «злочин як послуга» ще більше знижує бар'єр для входу фінансово мотивованих кіберзлочинців;

●***політичні та інші ідеологічні мотиви*****,** що обумовлюють до життя так званий *хактивізм* **–** використання комп'ютерів, комп'ютерних мереж для просування політичних ідей[2], в тому числі й втручання у виборчі процеси країн через використання технологій фреймингу, сугестії, чорного піару тощо. Керовані соціальними чи політичними мотивами, хактивісти використовують методи злому для просування своїх переконань або зриву діяльності організацій, з якими вони в опозиції, тощо. Їхні дії можуть варіюватися від спотворення вебсайтів, витоку даних[3] й до впливу на світогляд користувачів соціальних мереж, обумовлення їх вибору на користь соціально (зокрема політично) значущих дій;

●***помста:*** незадоволені співробітники або особи, які прагнуть помститися, скажімо колишньому роботодавцеві, можуть вдаватися до кібератак проти організацій або конкретних осіб;

●***ігрові мотиви.*** Деякі особи мотивовані складністю злому як виклику технічного, інтелектуального характеру, бажанням отримати визнання серед однолітків або просто заради розваги[4]. Скрипт-кідді часто потрапляють до цієї категорії. Це – термін, що використовується для зневажливої характеристики недосвідчених, низько кваліфікованих хакерів – «чорних капелюхів», які мають обмежені знання та здійснюють свої атаки за допомогою скриптів, створених іншими хакерами, а не розробляють власні. Часто мотивовані пошуком гострих відчуттів та популярністю серед своїх колег, ці хакери не становлять значної загрози для добре підготовленої організації»[5]. Але все ж скидати їх з рахунків не варто. Й деякі типові цифрові сліди здатні вказати саме не те, що в конкретному випадку діяв недосвідчений злочинець-гравець, для якого, зрештою, вчинення

[1] What is cyber crime? Types, examples, and prevention // CyberTalents. URL: https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention.

[2] Хактивізм // Вікіпедія – вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Хактивізм.

[3] What is Hacktivism: Types, Ethics, History & Examples / Imperva. URL: https://www.imperva.com/learn/application-security/hacktivism/

[4] Reynolds A. L. Profiling Cybercriminals: Behavioral Analysis and Motivations Behind Cybercrime Activities // *Cybersecurity Undergraduate Research Showcase*. 2024. URL: https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1094&context=covacci-undergraduateresearch

[5] Know Your Adversary: Understanding the Motivations of Different Types of Hackers // ERMProtect. URL: https://ermprotect.com/blog/know-your-adversary-understanding-the-motivations-of-different-types-of-hackers/?nowprocket=1.

кіберзлочину є способом задовольнити потребу у самоактуалізації, визнанні.

●***патріотично обумовлена діяльність проти ворожої держави, конкуруючої корпорації тощо.*** Держави чи конкуренти можуть займатися кібершпигунством для збору конфіденційної інформації з політичною, економічною чи стратегічною метою. Сюди можна віднести кібератаки під час збройних конфліктів, на кшталт агресивної війни росії проти України.

Мотивації часто корелюють з конкретними видами кіберзлочинів. Корислива мотивація тісно пов'язана з такими типами кіберзлочинів як фішинг, створення та поширення програми-вимагачів, незаконне заволодіння персональними даними[1]. Політичні мотивації керують хактивізмом і кібертероризмом. Помста часто лежить в основі особистісно забарвлених погроз, деяких видів цілеспрямованих атак на кібернетичну інфраструктуру. Організовані кіберзлочинні групи, як правило, керуються фінансовою вигодою, тоді як хактивістські групи мотивовані ідеологією. Державні суб'єкти переслідують геополітичні та стратегічні цілі. Кіберзлочинці часто мають кілька мотивацій, і вони можуть змінюватися з часом. Розуміння мотивацій, що стоять за кібератаками, є вирішальним для розробки ефективних стратегій кібербезпеки.

В основу типології кіберзлочинців також можна покласти характер їх технічних, технологічних знань і навичок. Відповідно – формуються такі кримінологічні типи:

– *скрипт-кідді:* їм бракує значних технічних знань, і вони покладаються на готові інструменти. Часто мотивовані гострими відчуттями або визнанням серед однолітків.

– *хакери-початквців («зелені капелюхи»):* новачки в хакерстві, але прагнуть навчатися та розвивати навички.

– *кваліфіковані хакери:* володіють значними технічними навичками. Кваліфіковані хакери можуть здійснювати складніші атаки, включаючи розгортання програм-вимагачів, витоки даних і складні фішингові кампанії[2]. «Чорні капелюхи» – використовують навички з кримінально протиправною метою, «сині» – це розробники програмного забезпечення, орієнтованого на безпеку (в тому числі від викриття правоохоронцями), а «червоні» – хакери-вігіланти[3], що самоправно переймають на себе функції держави як монополіста на легальне застосування сили в межах кримінальної юстиції.

– *елітні хакери* – професіонали найвищої категорії, творчі особистості, які нерідко виявляються розробниками ІТ-інновацій або ж, принаймні, неочікуваних напрямів, способів використання вже наявних розробок. Серед іншого елітні хакери можуть бути причетні до розробки складних стійких

[1] Arkvik I. What is financial cybercrime, and how can we prevent it? URL: https://www.visma.com/resources/content/what-is-financial-cybercrime-and-how-to-prevent-it.

[2] Borges E. Types of Cybercriminals and Their Motivations // Recorded Future. 2024. URL: https://www.recordedfuture.com/threat-intelligence-101/threat-actors/cybercriminals.

[3]What is Hacktivism: Types, Ethics, History & Examples / Imperva. URL: https://www.imperva.com/learn/application-security/hacktivism/

загроз (APT) або «експлойтів нульового дня» (недолік у безпеці програмного забезпечення, який невідомий тому, хто зацікавлений у його усуненні, наприклад, розробнику. «Експлойт нульового дня» – це метод, який хакери використовують для атаки на системи з раніше невідомою вразливістю)[1].

Типологія кіберзлочинців на основі особливостей цілепокладання дає можливості виділити такі їх типи:

– *одинаки, орієнтовані на особисті цілі.* Вони здійснюють атаки заради особистої вигоди: отримання важливої для них інформації, фінансових даних або переслідування[2];

– *підприємці (малі та великі).* Здійснюють кібератаки заради корпоративної (для групи осіб) фінансової вигоди. Невеликі об'єднання часто є вразливими через обмежені ресурси безпеки[3].

– *державні органи,* які організують атаки в межах здійснення актів диверсій, кібертероризму, вчинення воєнних кіберзлочинів. До цього переліку належать також атаки й на критичну інфраструктуру з метою зриву, саботажу або спричинення широкомасштабних негативних наслідків для цивільного населення. Щодо об'єктів, розташованих на території України, тільки за 2024 р. було скоєно 4365 кібератак, від якої страждала в першу чергу критична інфраструктура.

Цінність цілі є ключовим фактором у кіберзлочинній діяльності[4]. Взаємопов'язаність цифрових систем означає, що атаки на одну ціль можуть мати наслідки для інших наприклад атаки на ланцюг поставок, що призводить до зупинки всіє галузі. Заклади освіти мають унікальний набір вразливостей і цінних даних, що робить їх привабливими цілями[5].

Типологія на основі організаційної структури надає можливість вести мову про такі типи кіберзлочинів:

– *автономні злочинці*, що діють самостійно;

– *малі ситуативні групи,* що об'єднуються заради досягнення цілей протягом незначного проміжку часу. Є нестійкими;

– *організовані кіберзлочинні синдикати* – складні групи зі спеціалізованими ролями, часто схожі на легальний бізнес. Вони часто працюють з чітким розподілом праці, включаючи такі ролі, як

[1] Clough A. P. 3 Types of Cyber Threat Actors and Their Motivations // Risk & Insurance. 2022. URL: https://riskandinsurance.com/3-types-of-cyber-threat-actors-and-their-motivations/; Borges E. Types of Cybercriminals and Their Motivations // Recorded Future. 2024. URL: https://www.recordedfuture.com/threat-intelligence-101/threat-actors/cybercriminals

[2] Chen S., Hao M., Ding F., Jiang D., Dong J., Zhang S., Guo Q., Gao C. Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*. 2023. Vol. 10. № 1. P. 71. – DOI: 10.1057/s41599-023-01560-x.

[3] Common Targets for Cyberattacks in 2024 / IS Partners. 2024. URL: https://www.ispartnersllc.com/blog/common-targets-for-cyberattacks/

[4] Вахітова З. Теорія кіберрутинної діяльності // Оксфордська дослідницька енциклопедія кримінології. 2025. 22 січня. URL: https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-784.

[5] Miller E. The State of Higher Education Cybersecurity: Top Insights and Trends // BitLyft. 2023. URL: https://www.bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends/

тестувальники на проникнення, розробники шкідливого програмного забезпечення, переговорники та особи, які займаються відмиванням грошей[1];

– *публічно організовані суб'єкти* – групи, що фінансуються та керуються урядами країн.

– *хактивістські групи* – слабо організовані групи осіб, керовані політичними чи соціальними програмами. Є нестійкими, вразливими до викриття.

Висновки. У результаті проведеного дослідження встановлено, що сучасна кіберзлочинність, як кримінологічне явище, вимагає нового концептуального підходу до розуміння особи злочинця, яка діє в цифровому середовищі. Типологізація кіберзлочинців дозволяє систематизувати знання про їх соціально-психологічні характеристики, мотиваційні установки та моделі поведінки. З огляду на динамічність кіберсередовища, традиційні кримінологічні підходи до вивчення особи правопорушника потребують адаптації до нових форм девіантної активності.

З'ясовано, що більшість осіб, які вчиняють кіберзлочини, не мають кримінального минулого, мають високий інтелектуальний потенціал і, нерідко, працюють у легальному ІТ-секторі. При цьому зростає роль поведінкових та психофізіологічних характеристик у побудові ефективної профілактики кіберзлочинів.

Отже, особа комп'ютерного злочинця повинна стати одним із ключових об'єктів сучасних кримінологічних досліджень. Такий підхід сприятиме не лише глибшому розумінню цифрової злочинності, а й удосконаленню спеціальних та загальних заходів її запобігання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. … канд. юрид. наук : 12.00.08 / НАН України ; Інститут держави і права ім. В. М. Корецького. К., 2002. 212 с.

2. Борисова Л. В. Суб'єкт (особа) транснаціонального комп'ютерного злочину : криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права*. 2008. Вип. 44. С. 76–80.

3. Вахітова З. Теорія кіберрутинної діяльності // Оксфордська дослідницька енциклопедія кримінології. 2025. 22 січня. URL: https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-784.

4. Головкін Б. М. Теперішнє і майбутнє кримінології. *Проблеми законності*. 2020. № 149. С. 168–184.

5. Денисов С. Ф. Особа злочинця у кримінологічній теорії України. *Вісник Кримінологічної асоціації України*. 2020. № 1 (22). С. 152–159.

[1] Williams D. How High Level Cybercrime Groups Are Formed and Organized. URL: https://www.blackfog.com/how-high-level-cybercrime-groups-are-formed/

6. Кваша О. О. Організатор злочину кримінально-правове та кримінологічне дослідження. К. : Ін-т держави і права ім. В. М. Корецького, 2003. 216 с.

7. Конвенція про кіберзлочинність : Міжнародний документ Ради Європи. Конвенція від 23.11.2001 р. URL: : https://zakon.rada.gov.ua/laws/show/994_575#Text.

8. Костенко О. М., Перелигіна Р. В. Методологія і доктрина сучасної кримінології. К. : КУП НАН України, 2016. 115 с.

9. Кримінологія (Загальна частина) : навч. посіб. / [І. О. Бандурка, О. М. Литвинов, Ю. В. Орлов та ін.] ; за заг. ред. д-ра юрид. наук, проф. Ю. В. Орлова ; МВС України, Харків. нац. ун-т внутр. Справ Харків : ХНУВС, 2025. 616 с.

10. Кримінологія : підручник / А. М. Бабенко, О. Ю. Бусол, О. М. Костенко та ін.; за заг. ред. Ю. В. Нікітіна, С. Ф. Денисова. Є. Л. Стрельцова. 2-ге вид., перероб. і допов. Харків : Право, 2018. 416 с.

11. Лагода К. О., Орлов Ю. В. Невиконання судового рішення: кримінологічна характеристика та запобігіння : монографія / за заг. ред. О. М. Литвинова. Харків : ТОВ «В деле», 2016. 254 с.

12. Лисько Т. Д., Меланіч В. В., Славіта Ю. В. Протидія кіберзлочинності: сучасний стан вітчизняного законодавства та досвід зарубіжних країн. *Актуальні проблеми держави і права*. 2022. № 96. С. 44–49. DOI: https:// doi.org/10.32782/apdp.v96.2022.4.

13. Малій М. І. Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження : дис. ... канд. юрид. наук : 12.00.08. Хмельницький, 2021. 213 с.

14. Топчій В. В., Бодунова О. М. Система кримінальних правопорушень у сфері інформаційних технологій: міжнародно-правовий вимір. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 1 (10). С. 187–194.

15. Хактивізм // Вікіпедія – вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Хактивізм.

16. Чередниченко К. Ю. Кримінологічна типологія кіберзлочинців // Злочинці і жертви злочинів : матеріали XX всеукр. наук. конф. з кримінології для студентів, аспірантів та молодих вчених, м. Харків, 16 листоп. 2020 р. Харків, 2020. С. 711–716.

17. Albanese Jay S. A Typology of Cybercrime: An Assessment of Federal Prosecutions. *Journal of Criminal Justice and Law*. 2022. Vol. 6. Issue 1. URL: https://jcjl.pubpub.org/pub/vm45gchn/release/1.

18. Arkvik I. What is financial cybercrime, and how can we prevent it? URL: https://www.visma.com/resources/content/what-is-financial-cybercrime-and-how-to-prevent-it.

19. Borges E. Types of Cybercriminals and Their Motivations // Recorded Future. 2024. URL: https://www.recordedfuture.com/threat-intelligence-101/threat-actors/cybercriminals

20. Borges E. Types of Cybercriminals and Their Motivations // Recorded Future. 2024. URL: https://www.recordedfuture.com/threat-intelligence-101/threat-actors/cybercriminals.

21. Chen S., Hao M., Ding F., Jiang D., Dong J., Zhang S., Guo Q., Gao C. Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*. 2023. Vol. 10. № 1. P. 71. – DOI: 10.1057/s41599-023-01560-x.

22. Clough A. P. 3 Types of Cyber Threat Actors and Their Motivations // Risk & Insurance. 2022. URL: https://riskandinsurance.com/3-types-of-cyber-threat-actors-and-their-motivations/

23. Common Targets for Cyberattacks in 2024 / IS Partners. 2024. URL: https://www.ispartnersllc.com/blog/common-targets-for-cyberattacks/

24. Docs criminal justice glossary. Crime typologies. URL: https://docmckee.com/cj/docs-criminal-justice-glossary/crime-typologies-definition.

25. Introduction to Criminal Justice / Wesley B. Maier, Kadence C. Maier, William M., Terry D. Edwards. URL: https://openwa.pressbooks.pub/crimjust1/

26. Know Your Adversary: Understanding the Motivations of Different Types of Hackers // ERMProtect. URL: https://ermprotect.com/blog/know-your-adversary-understanding-the-motivations-of-different-types-of-hackers/?nowprocket=1.

27. Miller E. The State of Higher Education Cybersecurity: Top Insights and Trends // BitLyft. 2023. URL: https://www.bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends/

28. Reynolds A. L. Profiling Cybercriminals: Behavioral Analysis and Motivations Behind Cybercrime Activities // *Cybersecurity Undergraduate Research Showcase*. 2024. URL:

29. What is cyber crime? Types, examples, and prevention // CyberTalents. URL: https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention.

30. What is Hacktivism: Types, Ethics, History & Examples / Imperva. URL: https://www.imperva.com/learn/application-security/hacktivism/

31. Williams D. How High Level Cybercrime Groups Are Formed and Organized. URL: https://www.blackfog.com/how-high-level-cybercrime-groups-are-formed/

Стаття надійшла до редакції 10.07.2025

Petro P. HALUSHKO,
Postgraduate Student
(Kharkiv National University of Internal Affairs, Kharkiv, Ukraine)

CYBERCRIMINAL PERSONALITY: CRIMINOLOGY-TYPOLOGICAL CHARACTERISTICS

The article examines criminological approaches to the typology of

cybercriminals in the context of the rapid escalation of threats in the digital environment. The emphasis is on the need to rethink traditional provisions of criminological theory in the context of the post-industrial development of society, in particular due to the complexity of the structure of cybercrime and the growth of its impact on social relations. The importance of a deep analysis of the criminal's personality as a key element for the development of effective prevention measures is emphasized. The need to form a typology of cybercriminals is substantiated, which allows identifying common features, motives and behavioral models of persons committing criminal offenses in cyberspace. An overview of scientific approaches to the problem is provided, and the difficulties of identifying typical profiles of criminal offenders in connection with the specifics of cybercrime are analyzed. Particular attention is paid to the study of the personal, psychophysiological and social characteristics of cybercriminals.

Keywords: *cybercrime, criminological typology, criminal offender personality, computer crimes, digital environment, criminally unlawful behavior, psychological characteristics, counteraction to cybercrime.*