

УДК 343.22:343.3/.7:004

DOI <https://doi.org/10.24144/2307-3322.2025.89.3.62>

ОСОБА ЗЛОЧИНЦЯ ЯК ЕЛЕМЕНТ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КІБЕРЗЛОЧИНІВ

Пясковський В.В.,
*кандидат юридичних наук, професор,
професор кафедри криміналістики
навчально-наукового інституту права та психології
Національної академії внутрішніх справ
ORCID: 0000-0001-7954-1018
e-mail: pwwadd@gmail.com*

Куліуш В.М.,
*доктор філософії,
начальник управління протидії кіберзлочинам в м. Києві
Департаменту кіберполіції Національної поліції України
ORCID: 0009-0007-2131-1413
e-mail: viacheslav.kuliush@cyberpolice.gov.ua*

Курилін І.Р.,
*кандидат юридичних наук, доцент,
доцент кафедри криміналістики
навчально-наукового інституту права та психології
Національної академії внутрішніх справ
ORCID: 0000-0002-5672-3959
e-mail: ki3@ukr.net*

Пясковський В.В., Куліуш В.М., Курилін І.Р. Особа злочинця як елемент криміналістичної характеристики кіберзлочинів.

У науковій статті здійснено комплексне дослідження особи кіберзлочинця як одного з ключових елементів криміналістичної характеристики кіберзлочинів. Ураховуючи стрімкий розвиток цифрових технологій та зростання загроз у кіберпросторі, особливого значення набуває питання детального аналізу особистісних рис правопорушника, що діє в умовах віртуального середовища. У роботі акцентовано увагу на тому, що особа кіберзлочинця має низку специфічних соціально-демографічних, психологічних, поведінкових та мотиваційних характеристик, які відрізняють його від суб'єктів традиційної злочинності.

На підставі емпіричних досліджень визначено, що більшість кіберзлочинців – це чоловіки з певним рівнем технічної підготовки, з відповідною освітою або самостійно набутими знаннями в галузі інформаційних технологій. Водночас зростає частка осіб і без відповідної освіти, що засвідчує доступність інструментів для вчинення кіберзлочинів широкому колу користувачів. Звертається увага на такі психологічні риси кіберзлочинців, як антисоціальні нахили, логічне мислення, схильність до анонімності, високий інтелектуальний рівень, знижена емпатія. Показано, що вольова структура поведінки правопорушників, як і конкуренція мотивів під час прийняття рішень у кіберпросторі, істотно впливають на характер і складність вчинених діянь.

У статті аналізуються мотиваційні аспекти злочинної діяльності в кіберпросторі: від прагнення матеріальної вигоди до кібертероризму та самоствердження у відповідних соціальних спільнотах. Особливу увагу приділено формам і способам вчинення кіберзлочинів, включаючи використання шкідливого програмного забезпечення, анонімізаторів, віртуальних мереж тощо.

Авторами обґрунтовується, що комплексне розуміння особи кіберзлочинця відіграє важливу роль у формуванні криміналістичної методики розслідування кіберзлочинів, зокрема сприяє опе-

ративному встановленню кола підозрюваних, оцінці ризиків, прогнозуванню подальших дій злочинців та розробці ефективних заходів профілактики. Наукове дослідження особи кіберзлочинця поглиблює розуміння його місця в цифровому просторі й пропонує практичні підходи до підвищення ефективності боротьби з кіберзлочинністю.

Ключові слова: кіберзлочини, особа злочинця, криміналістична характеристика, кіберпростір, психологічний портрет, мотивація.

Pyaskovskyi V.V., Kuliush V.M., Kurylin I.R. The offender's personality as an element of the forensic characteristic of cybercrime.

This scientific article presents a comprehensive study of the cybercriminal's personality as one of the key elements of the forensic characteristic of cybercrimes. Given the rapid development of digital technologies and the growing threats in cyberspace, the issue of a detailed analysis of the personality traits of the offender operating in a virtual environment becomes increasingly relevant. The paper emphasizes that the cybercriminal possesses a number of specific socio-demographic, psychological, behavioral, and motivational features that distinguish them from subjects of traditional criminal activity.

Based on empirical research, it has been determined that most cybercriminals are men with a certain level of technical training, either possessing relevant formal education or self-acquired knowledge in the field of information technology. At the same time, the proportion of individuals without appropriate education is increasing, which indicates the accessibility of tools for committing cybercrimes to a wide range of users. Attention is drawn to psychological traits common among cybercriminals, such as antisocial tendencies, logical thinking, a preference for anonymity, high intellectual capacity, and reduced empathy. It has been shown that the volitional structure of offenders' behavior, as well as the competition of motives during decision-making in cyberspace, significantly influences the nature and complexity of the committed acts.

The article examines the motivational aspects of criminal activity in cyberspace, ranging from the pursuit of material gain to cyberterrorism and the need for self-affirmation within certain social communities. Particular attention is given to the forms and methods of committing cybercrimes, including the use of malicious software, anonymizing tools, virtual networks, and more.

The authors argue that a comprehensive understanding of the cybercriminal's personality plays a crucial role in developing forensic methods for investigating cybercrimes, particularly in identifying suspects, assessing risks, predicting further actions, and designing effective preventive measures. This research deepens the understanding of the offender's place in the digital domain and offers practical approaches to improving cybercrime counteraction.

Key words: cybercrime, offender's personality, forensic characteristic, cyberspace, psychological profile, motivation.

Постановка проблеми. У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації всіх сфер суспільного життя кількість кіберзлочинів, учинених в Україні, залишається стабільно високою з тенденцією до поступового зростання, що становить серйозну загрозу для безпеки громадян, суспільства та держави. Відповідно до статистичної інформації Офісу Генерального прокурора, загальна кількість облікованих злочинів (без урахування кримінальних проступків), передбачених ст.ст. 361–363¹ КК України, становила: 2020 року – 2 338; 2021 року – 3 126; 2022 року – 3 038; 2023 року – 3 240; 2024 року – 3 311 [1].

У зв'язку з цим виникає необхідність удосконалення діяльності правоохоронних органів з розслідування таких злочинів, зокрема, й шляхом поглибленого вивчення особи злочинця як одного з ключових елементів криміналістичної характеристики кіберзлочинів.

На відміну від традиційних форм злочинної діяльності, кіберзлочини часто вчиняються особами з високим рівнем технічної підготовки, специфічною мотивацією та особливостями поведінки, що потребує окремого аналізу. Незважаючи на актуальність цієї проблематики, питання криміналістичної характеристики особи кіберзлочинця досі не отримало достатнього теоретичного та прикладного опрацювання. Це зумовлює потребу у ґрунтовному дослідженні зазначеного питання з метою підвищення ефективності діяльності правоохоронних органів у виявленні, розслідуванні та попередженні кіберзлочинів.

У даній статті поставлено за мету визначити криміналістично значущі риси особи злочинця в системі криміналістичної характеристики кіберзлочинів, виявити типові риси, моделі поведінки

та соціально-психологічних особливості осіб, які вчиняють кіберзлочини, що дозволить в подальшому сформулювати на цій підставі рекомендації щодо підвищення ефективності розслідування та попередження таких злочинів.

Стан опрацювання проблематики. Питання криміналістичної характеристики злочинів, зокрема окремих її елементів, тривалий час перебуває в полі зору науковців. Значний внесок у розвиток теоретичних засад криміналістичної характеристики зробили такі вітчизняні дослідники, як А.Ф. Волобуєв, В.А. Журавель, О.М. Колесніченко, В.О. Коновалова, М.В. Салтевський, В.В. Тіщенко, С.С. Чернявський, В.Ю. Шепітько, Б.В. Щур та інші. Питання вивчення особи злочинця як елементу криміналістичної характеристики розглядалася ними в контексті розслідування окремих видів злочинів.

Разом із цим, питання, пов'язані з особливостями розслідування кіберзлочинів, розкриваються в працях таких дослідників, як А.С. Білоусов, А.І. Вознюк, М.І. Мотлях, Л.П. Паламарчук, О.А. Самойленко, О.С. Тарасенко, Д.М. Цехан та інших.

Комплексне вивчення особи злочинця саме в контексті кіберзлочинів як елементу криміналістичної характеристики залишається недостатньо розробленим, що свідчить про наявність наукової прогалини та актуальність подальшого дослідження у даному напрямі.

Виклад основного матеріалу. Згідно п. 7 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», кіберзлочин (або комп'ютерним злочин) визнається суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2]. Відповідальність за кіберзлочини передбачена в статтях 361–363¹ Кримінального кодексу України, що містяться в Розділі XVI Кодексу «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [3].

З огляду на законодавче закріплення поняття та встановлення відповідальності за кіберзлочини, постає питання не лише про їх правову кваліфікацію, а й про ефективні механізми їх розслідування та запобігання. Для цього необхідно виходити за межі суто нормативного аналізу та звернутися до глибшого осмислення кіберзлочинності як явища, що охоплює не лише правові, а й соціальні, психологічні та криміналістичні аспекти. У зв'язку з цим постає необхідність комплексного підходу до вивчення кіберзлочинності не лише як явища, що порушує інформаційну безпеку, а й як соціально-поведінкового феномена. Важливо розглядати не лише технічні аспекти вчинення таких злочинів, а й особистісні характеристики правопорушників, що суттєво впливають на способи реалізації злочинного наміру. Саме особа злочинця стає одним із ключових елементів, що дозволяє вибудовувати ефективну систему виявлення, розслідування та профілактики кіберзлочинів.

На нашу думку, вивчення особи кіберзлочинця як елемента криміналістичної характеристики кіберзлочинів, повинна передбачати аналіз таких складових, як соціально-демографічні ознаки, психологічні риси, мотиваційна сфера, а також форми протиправної діяльності.

В рамках нашого дослідження було вивчено 101 кримінальне провадження про злочини, передбачені Розділом XVI КК України за період часу з 2020 до 2025 роки. Результати дослідження дозволяють стверджувати, що переважна більшість осіб, які вчиняють кіберзлочини, – це чоловіки (70,3 %). У 97 % випадків вони є самоучками з різним рівнем комп'ютерної грамотності і лише 3 % мають спеціальну технічну освіту. На цій підставі, Д.М. Цехан, спираючись на узагальнення матеріалів національної судово-слідчої практики, справедливо, як на нашу думку, типізував осіб, які вчиняють кіберзлочини: користувач початкового рівня; звичайний користувач; упевнений користувач; досвідчений користувач; користувач-професіонал [4, с. 100–102]. Значна частина таких осіб працює у державному секторі (43,6 %) або є безробітними (40,6 %). Цікавим є той факт, що частка співробітників поліції, СБУ та військових, які вчинили кіберзлочини, склала 11,9 %, працівників банківської сфери – 8,9 %, а працюючі у сфері ІТ складають лише 1 %.

Результати наших досліджень певною мірою узгоджуються з висновками О.С. Тарасенка, який зазначає, що з розвитком комп'ютерних технологій та систем комунікації, їх агресивною ескалацією в усі сфери нашої життєдіяльності, все більш поширеним стає вчинення кіберзлочинів не фахівцями-комп'ютерщиками, а звичайними користувачами кібертехнологій. Досягнення у цій сфері уможливили вчинення кіберзлочинів не за допомогою відповідної освіти, багажу знань і навичок, а за допомогою відповідних керівництв та посібників [5, с. 207].

Для кіберзлочинців характерні антисоціальні або асоціальні риси, високий інтелектуальний рівень, схильність до маніпуляцій, анонімності, логічного мислення, а також знижений рівень емпатії. Такі особи демонструють вольову організацію поведінки, що проявляється у здатності до тривалого планування й реалізації складних злочинних схем.

Як вказує О.А. Самойленко, злочинцям, які діють у кіберпросторі, притаманний вольовий компонент людської психіки. Можна провести паралелі між вольовою дією особи та її злочинною діяльністю з використанням кіберпростору. По-перше, зловмисник змістовно вчиняє одиничний злочин шляхом елементарної вольової дії або комплекс органічно взаємопов'язаних злочинів шляхом складної вольової дії. По-друге, його діяльність завжди є вмотивованою, причому від складності кримінально протиправної діяльності в кіберпросторі залежить конкуренція мотивів вчинення. Наприклад, злочинець не зміг подолати всі технічні перешкоди на шляху отримання доступу до рахунків біржі криптовалют, тому опинився перед вибором виконати свій корисливий задум частково (заволодіти лише одним видом криптовалют) або пошкодити електронну систему біржі з метою помсти. Незаконно отримавши доступ до конфіденційної інформації, злочинець опиняється перед вибором: вчинити заплановане вимагання або інший злочин з її використанням (шахрайство, привласнення, незаконні дії з платіжними картками). Розв'язання проблеми конкуренції мотивів злочину нерозривно пов'язане з психологічними властивостями злочинця (психотипом). Тому доволі часто банківські установи, ІТ компанії, фірми охорони й технічного обслуговування, добираючи персонал, проводять тестування з метою визначення рівня професіоналізму, а також психотипу майбутнього працівника. Результати таких тестувань можуть бути цінними для працівників кіберполіції та слідчого під час первинної перевірки інформації з позицій визначення кола підозрюваних [6, с. 118].

Найбільш поширеним мотивом вчинення кіберзлочинів є матеріальна вигода (81,2 % таких злочинів, за результатами наших досліджень, було вчинено з корисливих мотивів): крадіжка фінансових даних, доступ до банківських рахунків, розповсюдження конфіденційної інформації і персональних даних. Водночас можуть спостерігатися хуліганські спонукання і навіть політичні чи ідеологічні мотиви, коли мова йде про кібератаки проти державних ресурсів (кібертероризм). За мотивацією майже всі вчені так чи інакше виділяють дві самостійні групи кіберзлочинців: корисливих злочинців і хакерів [7, с. 106]. У 4,9 % вивчених нами кримінальних провадженнях, осіб, які вчинили кіберзлочини, ми впевнено можемо назвати хакерами.

У кожному з цих випадків мотивація тісно пов'язана з потребою самоствердження, демонстрації переваги, досягнення певного статусу у хакерських спільнотах або форумах. Саме тому з метою ідентифікації у комп'ютерній мережі хакери дають собі клички-прізвиська, за якими вони відомі серед інших «колег» у хакерському співтоваристві (Scorpion, Bandito, Captain, King, Taran, Crazy та ін.), більшість з яких свідчить про моральні якості їх власників [8, с. 162]. Таким чином, мотиваційна структура особи кіберзлочинця поєднує як прагматичні цілі, так і глибинні психологічні потреби.

Кіберзлочини, як правило, вимагають тривалого планування та ретельної підготовки. Зловмисники використовують спеціальне програмне забезпечення, шкідливі скрипти, віруси, а також засоби маскування, зокрема VPN, TOR, проксі-сервери. Анонімність є ключовим фактором для уникнення викриття. Вона дає змогу не лише не бути ідентифікованим у певний момент, а й також, як наслідок, надавати про себе неправдиву інформацію, вступати в соціальну взаємодію, видаючи себе за іншу особу [9, с. 119].

Певного поширення набули групові форми злочинної діяльності – кіберзлочинні спільноти, члени яких розподіляють ролі та взаємодіють у віртуальному середовищі. Це ускладнює можливість встановлення їхнього реального місцезнаходження та ідентифікації. У 13,9 % вивчених нами кримінальних провадженнях, кіберзлочини були вчинені групою осіб, серед яких переважну більшість складають злочини, передбачені ст. 362 КК України (Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї) – 71,4 %.

Висновки. Результати проведеного дослідження свідчать про те, що особа злочинця є одним із ключових елементів криміналістичної характеристики кіберзлочинів, що безпосередньо впливає на побудову ефективної методики їх розслідування. З урахуванням специфіки злочинної діяльності, особи, які її вчиняють, зазвичай мають певний рівень технічної підготовки, діють у віртуаль-

ному просторі, можуть діяти анонімно та часто не підпадають під традиційні криміналістичні типології злочинців. Це потребує формування нових підходів до аналізу соціально-демографічних, психологічних та поведінкових характеристик таких осіб.

Встановлення типових рис особи кіберзлочинця сприяє не лише ідентифікації правопорушника, а й удосконаленню способів встановлення мотивів протиправної поведінки та прогнозування подальших дій. Особа кіберзлочинця – не лише об'єкт дослідження, а й ключ до побудови дієвих криміналістичних моделей, що допомагають адаптувати методику розслідування до новітніх викликів цифрової епохи. Отже, включення результатів детального аналізу особи злочинця до структури криміналістичної характеристики кіберзлочинців є важливим чинником підвищення ефективності діяльності правоохоронних органів у боротьбі з кіберзлочинністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Звіт Офісу Генерального прокурора про зареєстровані кримінальні правопорушення та результати їх досудового розслідування за 2020–2024 рр. Офіс Генерального прокурора: [сайт]. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2> (дата звернення 06.05.2025).
2. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення 06.05.2025).
3. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення 06.05.2025).
4. Кіберзлочинність та електронні докази: навчальний посібник / Б.М. Головкін, О.І. Денькович, В.В. Луцик, Д.М. Цехан; за ред. О. Денькович, Г. Шмельцер. Електрон. вид. Львів: ЛНУ ім. Івана Франка, 2022. 298 с.
5. Тарасенко О.С. Характеристика осіб та злочинних угруповань, які вчиняють кримінальні правопорушення, пов'язані з обігом протиправного контенту в мережі інтернет. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2022. С. 206–213.
6. Самойленко О.А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А.Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.
7. Піцик Ю.М. Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності в кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету*. Сер.: Юриспруденція. 2017. № 26. С. 105–107.
8. Титаренко А.В. Особа кіберзлочинця як елемент криміналістичної характеристики. *Журнал східноєвропейського права*. 2019. № 62. С. 159–168.
9. Швець Д.В. Підходи до визначення психологічного портрета кіберзлочинця. *Актуальні питання протидії злочинності та торгівля людьми*: зб. матеріалів всеукр. наук-прак. конф. Харків, 23 листопада 2018 р. Харків: ХНУВС, 2018. С. 118–121.