

**Лефтеров Л. В.,**  
*начальник відділу управління  
інформаційних технологій і програмування в Південному регіоні  
Департаменту кіберполіції Національної поліції України*

## КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ОСІБ, ПІДОЗРЮВАНИХ У КІБЕРЗЛОЧИНАХ

**Анотація.** У статті проведено кримінологічний аналіз осіб, які скоюють злочини із використанням комп'ютерних мереж. За результатами проведеного дослідження встановлено, що більшість підозрюваних у кіберзлочинах – це чоловіки віком 20–35 років із переважно середньо-спеціальною та середньою освітою, досвідом самонавчання у галузі високих інформаційних технологій. З'ясовано, що кіберзлочинцям загалом притаманні певні риси корисливих та ігрових типів злочинців і шахраїв, але у них можуть бути відсутні акторські здібності, навички вербального спілкування, натомість кіберзлочинці можуть мати спеціальні технічні знання, різні особистісні комплекси та ілюзії. За результатами дослідження розроблено «Типовий портрет кібершахрая».

**Ключові слова:** кримінологічна характеристика, особистість кіберзлочинця, комп'ютерні мережі, Інтернет, портрет кібершахрая.

**Постановка проблеми.** Всебічний кримінологічний аналіз злочинів, скоєних із використанням комп'ютерних мереж, та розробка ефективних шляхів і напрямів їх запобігання та профілактики неможливі без урахування суб'єктивно-особистісних характеристик осіб, які безпосередньо скоюють кіберзлочини та шахрайства. Злочини, які скоєні із використанням комп'ютерів та Інтернету, зазвичай мають відношення до злочинності, спрямованої проти власності або держави, однак разом із цим визнаються кіберзлочинами і вчиняються особами, які мають свої суб'єктивні особливості і можуть відрізнятися від інших категорій і типів злочинців.

**Стан дослідження.** Вчення про особу, підозрювану у скоєнні злочину, та власне особистість злочинця є одним з основних складників предметної галузі кримінологічної науки та дає змогу з'ясувати всі інші кримінологічні проблеми, будь-то детермінанти злочинності або організація боротьби з нею. Не випадково проблематиці вивчення особистості злочинця значну увагу приділяли представники класичних кримінологічних шкіл. Так, Ч. Беккарія, І. Бентам, Ф. Лист, Л. Фейербах та інші вчені вже у XVIII – XIX століттях рішуче відкинули теологічне розуміння злочинності як прояву «сатанинського», диявольського початку. На їхню думку, злочин – це наслідок свідомої поведінки людини, яка, володіючи повною свободою волі, здійснює вибір варіанта своїх дій [1].

Сучасні дослідники торкаються різних аспектів особистості злочинця, зокрема М.О. Кравцова надає кримінологічну характеристику особистості кіберзлочинця. За її дослідженнями, кіберзлочинці – це переважно працездатні, але непрацюючі, неодружені чоловіки, в структурі морально-психологічних якостей яких превалюють корисливість, правовий нігілізм, поєднані з детермінованим специфікою кіберпростору комплексом

сваволі та ілюзій [2]. Проте у зв'язку із подальшим зростанням кількості та варіативності злочинів із використанням комп'ютерних мереж нині актуалізуються подальші кримінологічні дослідження особистості кіберзлочинця.

**Метою статті** є здійснення кримінологічної характеристики кіберзлочинців на підставі дослідження осіб, які підозрюються у скоєнні злочинів із використанням комп'ютерних мереж, а також розробка типового портрета кібершахрая.

**Виклад основного матеріалу.** Досліджуючи осіб, які скоюють злочини з використанням комп'ютерних мереж, їх можна розглядати як з точки зору характеристики злочинних дій, так і з боку характеристики особистості – суб'єктів скоєння злочинів. Так, фахівцями університету Норідж (приватний військовий університет, розташований у Нортфілді, штат Вермонт, США), виділяються такі види кіберзлочинців:

- ідентифікаційні злодії, як правило, – це кіберзлочинці, які намагаються отримати доступ до особистих даних жертв (ім'я, адресу, номер телефону, місце роботи, банківський рахунок, інформацію про кредитні картки та номер соціального страхування) та використовують цю інформацію для здійснення фінансових операцій, видавши себе за потерпілого;

- «інтернет-сталкери» – це категорія кіберзлочинців, які зловмисно контролюють діяльність своїх жертв в Інтернеті. Ця форма злочинності ведеться через використання соціальних мереж та шкідливих програм, які здатні відслідковувати комп'ютерну активність особистості з дуже малим виявленням;

- «пікери» (або шахраї, «фішери») – категорія кіберзлочинців, які намагаються отримати особисту або конфіденційну інформацію через комп'ютери жертв, це часто здійснюється через «фішингові» веб-сайти;

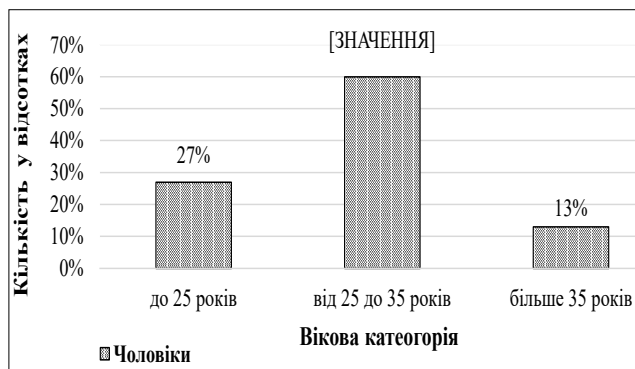
- кібертерористи – це добре розвинена, політично натхненна категорія злочинців, учасники якої намагаються викрасти дані та/або компрометувати корпоративні чи державні комп'ютерні системи та мережі, завдаючи шкоди країнам, підприємствам, організаціям або окремим особам [3].

Мотивуючими чинниками для кіберзлочинців зазвичай визначаються: досягнення грошової вигоди; шпигунство; саботаж політичних або релігійних переконань; цікавість; прагнення до гострих відчуттів, сексуальних імпульсів; нетерпимість; підвищення самооцінки та намір щодо контролю та маніпуляції оточуючими. Іноді у такого виду злочинців фіксуються нарцисизм та інші психопатії. Р. Мітчелл визначив типи кіберзлочинців, які відрізняються своїм рівнем майстерності та мотивацією, зокрема це такі: початківці; кіберпанки; внутрішні (внутрішня загроза); кодери; інформаційні воїни/кібертерористи; старі хакери охорони; професійні кіберзлочинці [4].

Є загальне хибне уявлення щодо кіберзлочинців. Передбачається, що вони мають різноманітні навички та злочинний досвід,

який дає змогу їм ініціювати широкий спектр нападів, згодом заробляючи величезну кількість грошей. Насправді, нещодавні дослідження, проведені серед членів закритої підпільної спільноти, показали, що більшість кіберзлочинців заробляють від 1000 до 3000 доларів США на місяць, а лише 20% заробляють значно більшу суму в розмірі \$ 20 000 на місяць та більше [5].

З метою здійснення кримінологічної характеристики комп'ютерних злочинів нами було проведено дослідження з використанням джерел, що є у відкритому доступі в мережі Інтернет стосовно злочинців, які розшуковуються за даними Федерального бюро розслідування (далі – ФБР) США. Повний перелік осіб, що складається із 42 підозрюваних, які розшуковуються ФБР за підозрою у скоєнні кіберзлочинів, зазначається на відповідному сайті «Найрозшукуваніші злочинці» [6]. За результатами проведеного дослідження виявлені соціально значимі ознаки міжнародного кіберзлочинця. Так, за критерієм віку встановлено, що більшість осіб (60%), які перебувають у федеральному та міжнародному розшуку, віком від 20 до 35 років, за статевою ознакою досліджувані підозрювані у кіберзлочинах – чоловіки (рис. 1).



**Рис. 1. Віковий діапазон осіб, які перебувають у федеральному та міжнародному розшуку ФБР США за скоєння кіберзлочинів**

Слід зазначити, що список кіберзлочинців за версією ФБР включає в себе справді особливо небезпечних правопорушників, які завдали значної фінансової шкоди корпораціям або державі, компрометували системи інформаційної безпеки низки Національних агенцій та порушували діяльність інформаційно-технічного ресурсу, проте діяльність більшості з них була спрямована стосовно Сполучених Штатів Америки. Крім того, у списку відсутні безпосередньо громадяни США [6]. Тому здійснити об'єктивні висновки за територіальними ознаками особистості кіберзлочинців вкрай складно. Однак, посилаючись на вказані дані, все ж таки можна з певною ймовірністю підтвердити той факт, що більшість злочинців є громадянами держав, в яких присутній низький рівень протидії кіберзлочинам, це – держави Середнього, Далекого Сходу (Пакистан, Індія, Іран, Сирія, В'єтнам тощо). Також вагомими є політичні фактори – відношення тієї або іншої держави до діючого уряду США, що зумовило велику кількість підозрюваних у кіберзлочинах з Північної Кореї, Російської Федерації та Китаю.

За аналогією з проведеним аналізом стосовно міжнародних кіберзлочинців за версією ФБР США нами було здійснено дослідження щодо громадян України, які були підозрюваними за скоєння шахрайств з використанням комп'ютерних мереж. Дослідження проводилось стосовно осіб, яким оголошено про

підозру за скоєння злочинів, передбачених ч. 3, 4 ст. 190 КК України [7], на підставі даних з інтегрованої інформаційно-пошукової системи Міністерства внутрішніх справ України «Армор», функціонування якої регламентовано відповідним наказом МВС України [8]. Встановлено, що протягом 2017 року підрозділами Департаменту кіберполіції Національної поліції України розкрито шахрайств, вчинених шляхом незаконних операцій із використанням електронно-обчислювальної техніки, за 1851 кримінальними провадженнями, оголошено про підозру 210 окремим особам.

Аналіз даних дав змогу визначити тенденції злочинності (шахрайства, вчиненого з використанням комп'ютерних мереж) за статевою ознакою. Так, 72% кримінальних проваджень (за ознаками ч. 3 та ч. 4 ст. 190 КК України) відкриті стосовно чоловіків та 18% щодо жінок. Таким чином, встановлено, що вказана категорія кіберзлочину вчиняється переважно чоловіками, однак існує відсоток і жінок. Крім того, доцільно додати ще один критерій – злочини, що скоєні за співучастю особами чоловічої та жіночої статі (10%).

Кібершахрайство має безпосереднє відношення до сегмента інформаційних технологій (ІТ). А згідно з даними «зарплатного опитування DOU» (проводилось з 12 червня по 12 липня 2017 року анонімно, в якому взяли участь 8704 особи), жінок, які працевлаштовані або перебувають у статусі вільного працівника у сфері інформаційних технологій станом на 2017 рік, лише 20% [9]. Зазначені дані вказують на рівень залученості жінок у технічній сфері, що тотожно навчанню у технічних вищих навчальних закладах або в технічній підтримці того чи іншого державного і приватного підприємства. Однак, згідно з тими самими результатами вищезазначеного опитування, тенденція збільшення з кожним роком кількості осіб жіночої статі у сфері ІТ становить у середньому 2%. Так, у 2011 частка жінок із вказаними інтересами становила лише 7%.

За результатами дослідження вікового діапазону українських підозрюваних у кібершахрайстві встановлено, що в 2017 році злочини скоювали громадяни віком від 17 до 61 року, тобто від підлітків до осіб пенсійного віку. Крім того, виявлено факт, що більший відсоток становлять особи у віковому діапазоні від 20 до 35 років, що співпадає із наведеним вище дослідженням стосовно осіб, які розшуковуються ФБР США за підозрою у скоєнні кіберзлочинів. З досліджуваної категорії підозрюваних осіб лише 26% мали одну чи більше вищих освіт, 21% – особи, що мали середньо-спеціальну освіту. Більшість кібершахраїв мали повну середню освіту, однак це аж ніяк не значить, що українська шкільна програма містить основи щодо скоєння шахрайств із використанням комп'ютерних мереж. Посилаючись на вказаний вище факт, доцільно зробити висновок, що особою кіберзлочинця вказаної категорії здебільшого є людина, яка самостійно отримує або вже здобула освіту у сфері високих інформаційних технологій (комп'ютерної безпеки, програмування, сучасних тенденцій розвитку комп'ютерних мереж) поза будь-яким вищим навчальним закладом, без педагогічної допомоги.

Що стосується національної приналежності, то серед осіб, що вчинили шахрайства з використанням електронно-обчислювальної техніки, відсутня перевага осіб тієї або іншої національності, тобто національний склад злочинців загалом відбиває етнічний склад України. Аналіз місць мешкання кібершахраїв засвідчив, що 67% з них були вчинені громадянами за місцем свого проживання (на території окремої області).

За 32% кримінальними провадженнями оголошено про підозру особам, які скоїли злочин не за місцем мешкання (реєстрації). Лише в 1% випадків злочини були скоєні громадянами іншої держави або особами без громадянства.

Вказані соціально-демографічні ознаки кібершахраїв являють лише зовнішню характеристику. Для уявлення про внутрішній світ осіб, що скоїли злочин, необхідне вивчення їхніх особистісних особливостей. До цих властивостей особистості відносяться спрямованість, риси характеру, моральні якості, знання, навички, звички, рівень особистої культури тощо. Морально-психологічні якості кібершахраїв у цілому є ідентичними характеристикам шахраїв загальнокримінальної спрямованості.

Найбільш притаманними психологічними особливостями шахраїв, за даними сучасних досліджень, є певні мотиви злочинної поведінки – жага наживи, жадібність, прагнення придбати матеріальні блага і схильність до легкого життя, більш високий рівень інтелекту (зокрема, порівняно з іншими категоріями злочинців), вміння швидко пристосовуватися до сучасних умов життя, холоднокровність, розважливості, здатність володіти собою, вміння зрозуміти психологію іншої людини і викликати до себе довіру, демонстрація співчуття і співпереживання, акторські здібності, спостережливість, розкутість поведінки, готовність використовувати обман, прагнення до паразитизму, моральна розбещеність, лицемірство, нахабність і грубість, володіння прийомами психологічного впливу на іншу людину та інших особливостей [10].

Однак, на нашу думку, кібершахрайство – особлива категорія злочину, яка змінила поняття та деякі принципи обману та зловживання довірою. Так, сучасний кібершахрай може бути таким, у якого відсутні акторські здібності, він взагалі може не показувати свою поведінку, в нього можуть бути не розвинені навички й уміння вербального спілкування.

З огляду на те, що провідне місце серед стійких психологічних особливостей особистості займають мотиви шахрая, як і кібершахрая, властиві прагнення до самоствердження на соціально-психологічному рівні (пов'язано з потребою домогтися визнання з боку найближчого оточення – сім'ї, друзів, знайомих, колег по роботі) і на індивідуальному рівні (пов'язано з бажанням підвищити самооцінку і посилити самоповагу шляхом здійснення вчинків, що сприяють, на думку особистості, подоланню будь-яких психологічних слабкостей). Не менш типовими для кібершахраїв є ігрові мотиви, властиві особам, які скоюють злочини не тільки і не стільки з метою отримання матеріальної вигоди, а скільки заради гри та ризику, для отримання гострих відчуттів. Досить яскраво ці мотиви виявляються в ситуаціях, в яких здійснюється інтелектуальне протиборство і змагання в спритності, де потрібні кмітливість, уміння максимально використовувати сприятливі обставини і швидко приймати рішення.

За результатами попередніх та власних досліджень нами розроблено «Типо-

вий портрет особистості кібершахрая», який наочно подано на рис. 2.

Структуровані складники психологічного портрета кібершахраїв вказують на певну антисуспільну й егоїстичну особистісну спрямованість і підкреслюють проблему ускладнення психодіагностики шахрайських поведінкових проявів та їх логіки доказування. За кримінально-правовими ознаками осіб, які вчиняють кібершахрайства, важливим фактом є сукупність злочинної діяльності. Суттєвими умовами і факторами для розвитку вказаної категорії злочинності можна вважати віктимність та необізнаність потерпілих осіб, що потребує окремого дослідження.

**Висновки.** Таким чином, узагальнюючи проведений кримінологічний аналіз осіб, які скоюють злочини з використанням комп'ютерних мереж, слід визначити такі закономірності:

- більшість підозрюваних за кіберзлочини, які перебувають у міжнародному розшуку, – це чоловіки віком 20–35 років, значна кількість таких злочинців є громадянами держав, в яких присутній низький рівень протидії кіберзлочинам (країни Середнього, Далекого Сходу).
- більшість громадян України, які були підозрюваними за скоєння шахрайств, скоєних із використанням комп'ютерних мереж, також були особами чоловічої статі, але кримінальні провадження за кібершахрайство відкривались також і щодо жінок та за співучастю особами чоловічої та жіночої статі;
- чверть підозрюваних кібершахраїв мали вищу освіту, інші мали середньо-спеціальну та середню освіту;
- більшість кібершахраїв самостійно отримують освіту та досвід у сфері високих інформаційних технологій (комп'ютерної безпеки, програмування тощо) поза навчальним закладом, без педагогічної допомоги, це зумовлює, що особи кібершахраїв здебільшого мають спеціальні технічні знання, однак чимала частка з них може і не мати таких знань і досвіду, що є причинами скоєння злочинів у складі групи;

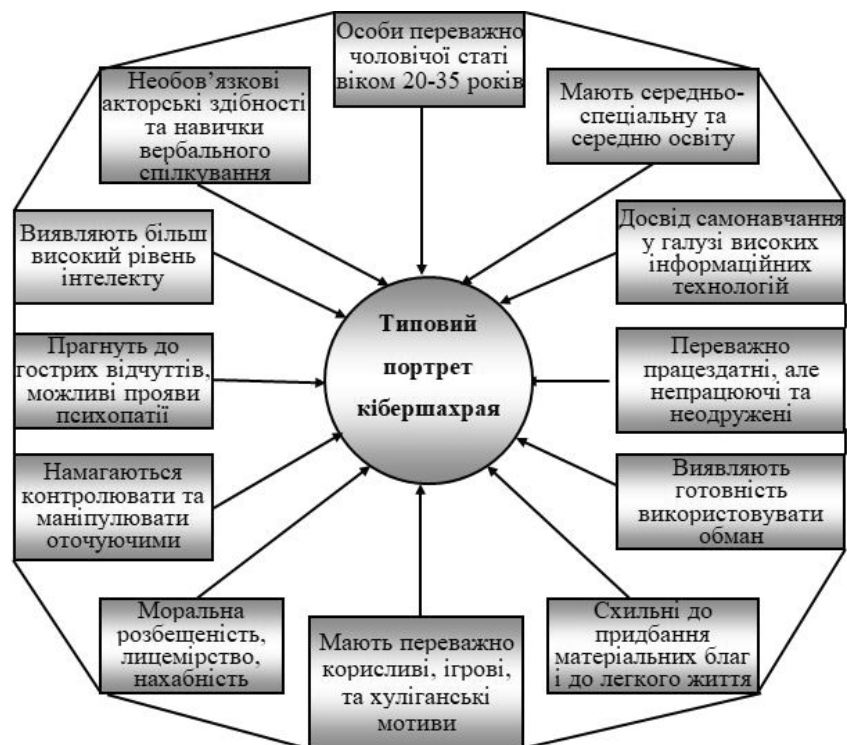


Рис. 2. Типовий портрет особистості кібершахрая

– шахраям у сфері кіберзлочинності притаманні соціально-демографічні і психологічні ознаки, схожі зі злочинцями у напрямі шахрайства загальнокримінальної спрямованості, проте кіберзлочинність – це особлива категорія злочину, яка змінила поняття та деякі принципи обману та зловживання довірою. Так, сучасний кібершахрай може бути таким, у якого відсутні акторські здібності, він взагалі може не показувати свою поведінку, в нього можуть бути не розвинені навички й уміння вербального спілкування, проте виявлятися певні особистісні комплекси та ілюзії.

#### *Література:*

1. Класичне і антропологічне спрямування кримінологічних теорій. URL: <http://um.co.ua/3/3-6/3-68855.html>
2. Кравцова М.О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Харків, 2016. С. 20.
3. Who Are Cyber Criminals? Academic Programs & Resources. Information Security & Assurance by Norwich University Online. February 13th, 2017. URL: <https://online.norwich.edu/academic-programs/masters/information-security-assurance/resources/articles/who-are-cyber-criminals>
4. Profiling the Cybercriminal. URL: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/profiling-cybercriminal>
5. Barysevich A. Inside the Mind of Cybercriminals. URL: <https://www.recordedfuture.com/cyber-criminal-profiling/>
6. Cyber's Most Wanted. URL: <https://www.fbi.gov/wanted/cyber>
7. Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст. 131.
8. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: наказ МВС України від 12 жовт. 2009 року № 436.
9. Женщины в IT: портрет, планы, мотивация. URL: <https://dou.ua/lenta/articles/it-woman/>
10. Борисова С.Е. Психологические особенности лиц, совершивших мошенничество, и их учет при расследовании преступлений. Прикладная юридическая психология, № 1, 2008. С. 108–115.

#### **Лефтеров Л. В. Криминалистическая характеристика лиц, подозреваемых в киберпреступлениях**

**Аннотация.** В статье проведен криминалистический анализ лиц, совершающих преступления с использованием компьютерных сетей. По результатам проведенного исследования установлено, что подавляющее большинство подозреваемых в киберпреступлениях – это мужчины в возрасте 20–35 лет с преимущественно средне-специальным и средним образованием, опытом самообучения в области высоких информационных технологий. Выяснено, что киберпреступникам в целом присущи определенные черты корыстных и игровых типов преступников и мошенников, но у них могут отсутствовать актерские способности, навыки вербального общения, вместе с тем киберпреступники могут иметь специальные технические знания, различные личностные комплексы и иллюзии. По результатам исследования разработан «Типовой портрет кибермошенника».

**Ключевые слова:** криминалистическая характеристика, личность киберпреступника, компьютерные сети, Интернет, портрет кибермошенника.

#### **Lefterov L. Criminological characteristics of persons suspected of cyber crimes**

**Summary.** Criminological analysis of persons committing crimes using computer networks has been carried out. According to the results of the study, it was found that the overwhelming majority of suspected cybercriminals are men aged 20–35, with predominantly secondary education, they receive education and experience in the field of high-level information technologies in self-education manner. It is revealed that cybercriminals generally have certain features of profit and game types of criminals and swindlers, but they may not have the actor's abilities, skills of verbal communication, whereas cybercriminals may have special technical knowledge, different personal complexes and illusions. According to the results of the study "A typical portrait of a cybercrook" was developed.

**Key words:** criminological characteristic, personality of cybercriminal, computer networks, Internet, portrait of cybercrook.