УДК 343.9:343.7:004.056 *DOI: https://doi.org/10.32631/vca.2025.1.17*

Олексій Олександрович ДЕРЕВЯГІН,
кандидат юридичних наук,
старший науковий співробітник
(Харківський національний університет внутрішніх справ, м. Харків)

Дмитро Валентинович ПАШНЄВ,
кандидат юридичних наук, доцент
(Харківський національний університет внутрішніх справ, м. Харків)

Антон Олександрович НОВИЦЬКИЙ,
доктор філософії
(ГУНП в Харківській області, м. Харків)

ОКРЕМІ ПІДХОДИ ДО ВИЗНАЧЕННЯ СУЧАСНОГО ПОРТРЕТУ ПРОФЕСІЙНОГО КІБЕРШАХРАЯ

У статті на підставі аналізу праць вітчизняних й іноземних учених, присвячених кримінологічним, криміналістичним, а також соціально-психологічним характеристикам осіб, які вчиняли кібершахрайства, запропоновано типологію сучасного портрету професійного кібершахрая відповідно до ознак шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки, що є суттєвим внеском

в убезпечення життєдіяльності людини, громадянина, органів місцевого самоврядування, державних органів та світового суспільства загалом від кримінальних проявів в кіберпросторі.

Запропоновані особливості сучасного портрету професійного кібершахрая є підґрунтям для вдосконалення методики розслідування кримінальних правопорушень досліджуваної категорії, визначення тактики проведення слідчих (розшукових) та негласних слідчих (розшукових) дій, застосування оперативно-розшукових можливостей зокрема використання конфіденційного співробітництва під час здійснення оперативного супроводження кримінального провадження, організації заходів протидії та превенції шахрайств, вчинених шляхом незаконних операцій з використанням електронно-обчислювальної техніки.

Ключові слова: *кіберзлочинність, кібершахрайство, кібершахрай, типологія, незаконні операції, електронно-обчислювальна техніка (ЕОТ).*

Постановка проблеми. Загрозливі темпи росту рівня кібершахрайств, викликані глобальним розширенням всього спектру інформаційних технологій із застосуванням штучного інтелекту, створюють новітні загрози та виклики для світового співтовариства. Внаслідок цього виникають практичні завдання і у сфері протидії кіберзлочинності, які вимагають постійного наукового супроводження та оперативного розв'язання. В цьому аспекті напрацювання кримінологічної науки виступають ключовим інструментарієм для застосування всіх наявних можливостей системи запобігання кримінальній протиправності.

Оскільки українське інформаційне суспільство є невід'ємною складовою всесвітнього кіберпростору, через який відкриваються транснаціональні віртуальні межі, постає необхідність унормування всіх процесів, що там відбуваються, у сучасному національному та міжнародному законодавствах. Зазначене передбачає формування на рівні держави національного інформаційного суспільства, яке консолідує взаємодію різних верств населення, підприємств, установ, організацій, органів державної влади та місцевого самоврядування з використанням інформаційних технологій grid і blockchain.

Результати аналізу досягнень нового світового ладу – електронної цивілізації – свідчать про наявність не лише позитивних звершень, але й численних реальних ризиків, загроз, кібератак і небезпек, зокрема, формування потужної новітньої організованої міжнародної (транскордонної, транснаціональної та трансконтинентальної) кіберзлочинності. Відтак постає необхідність у детальному дослідженні, пов'язаному з вивченням характерних рис, ознак і специфічних особливостей типології сучасного портрету професійного кібершахрая.

Особа правопорушника є об'єктом дослідження кримінології, криміналістики, юридичної психології та інших наук. Її вивчали такі вчені: О. Бабенко, О. Бишевець, А. Волобуєв, О. Дудоров, М. Зубань, О. Колесниченко, А. Мокляк, С. К. Науменко, В. Пивоваров, О. Самойленко,

В. Тіщенко, О. Ткачова, А. Толкач, І. Харитоненко, В. Шепітько, Ю. Шемшученко та ін. Однак питання вчинення кібершахрайства, шляхом незаконних операцій з використанням електронно-обчислювальної техніки (далі – ЕОТ) досліджено недостатньо. Тому розслідування таких кримінальних правопорушень проводять в умовах інформаційної недостатності. Це засвідчує необхідність удосконалення правоохоронної діяльності з позиції висвітлення відомостей про особу сучасного професійного кібершахрая.

Окресленням проблемних питань щодо суб'єктів кримінальної протиправної діяльності, які здійснюють кримінальні правопорушення у сфері використання мережі Інтернет, зокрема шляхом незаконних операцій з використанням ЕОТ, розглядали у своїх роботах вітчизняні науковці: П. Андрушко, Л. Борисова, О. Брисковська, П. Біленчук, С. Лозова, М. Малій, М. Омельяненко, Ю. Піцик, Т. Романенко, М. Чаплик, С. Чернявський, Д. Швець та ін.

Попри безумовну теоретичну та практичну важливість цих досліджень, окреслену тематику комплексно не було розглянуто, суб'єктивно особистісні властивості сучасного портрету професійного кібершахрая вивчено недостатньо, що ускладнює процес розслідування кримінальних правопорушень щодо шахрайств, вчинених шляхом незаконних операцій з використанням ЕОТ.

Подальше дослідження та розроблення типології сучасного портрету професійного кібершахрая є актуальним і становить не лише теоретичне, а й практичне значення. Це дає можливість визначення соціально-психологічних даних про особу кібершахрая, що є одним із головних факторів як під час розслідування шахрайств, вчинених шляхом незаконних операцій з використанням ЕОТ, так і в ході організації заходів протидії таким кримінальним правопорушенням та їх превенції.

Мета статті полягає у визначенні типології сучасного портрету професійного кібершахрая з метою удосконалення протидії шахрайствам, вчиненим шляхом незаконних операцій з використанням ЕОТ.

Виклад основного матеріалу. Здійснені сучасні різнобічні узагальнення поняття сучасного портрету професійного кібершахрая підтверджують ствердження про те, що в юридичній літературі і в правозастосовній діяльності доцільно застосовувати термін «кібершахрай», оскільки термін «кіберзлочинець» доречний відносно конкретної особи лише після визнання її винною не інакше як тільки за вироком суду. Відзначимо, що в результаті вивчення досвіду практичної діяльності правоохоронних органів, проведеного соціально-правового, психолого-кримінологічного та експертно-криміналістичного аналізу (1989–2024 рр.), спираючись на дослідження проведені П. Д. Біленчуком[1], М. І. Малієм[1],

[1] Біленчук П. Д., Малій М. І. Пріоритетні напрями досліджень психологічного портрету електронного зловмисника. *Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів*: зб. тез Міжнар. наук.-практ. конф. (м. Київ, 30 жовтня 2020 р.). Київ, ДНДІ МВС України, 2020. С. 79-81.

О.М. Брисковською[2] та іншими вченими щодо характеристики особи комп'ютерного злочинця, можна стверджувати, що серед сучасних професійних кібершахраїв переважна більшість становлять особи чоловічої статі. Водночас наявна слідча і судова практика підтверджують стрімке зростання в структурі кібершахрайств представниць жіночої статі, так званих кібершахрайок. Це також підтверджується статистичними даними. Так, більшість кіберзлочинів проти власності, які займають 79 % їх структури, – це шахрайства, учинені чоловіками (94 %). Такі кримінальні правопорушення вчиняються переважно особами, які офіційно не перебувають у шлюбі та не мають дітей. Кількість неодружених осіб становить 70 %, одружених – 30 %. Згідно з даними судової практики, близько 50 % осіб, які вчинили кіберзлочини, не мають постійного місця роботи, що зазвичай і є причиною вчинення шахрайства. Серед решти більшість становлять менеджери нижчої та середньої ланок, рідше – службові особи та програмісти. Якщо середній вік звичайного шахрая становить 26–39 років, то середній вік кібершахрая – від 22 до 42 років, а соціальне становище в суспільстві варіюється від студента до співробітника державної установи або фірми[3].

Проведений системний аналіз психофізіологічних характеристик дає можливість охарактеризувати таку особу як працівника, який вражає своєю індивідуальністю, аналітичним мисленням і творчими здібностями, який є фахівцем у своїй галузі, спроможний долати технологічні виклики будь-якої складності, що робить його привабливим для працевлаштування. Філософські концепції в поєднанні з високим інтелектом дають такій особі можливість обґрунтовувати будь-які кримінальні задуми, позиціонувати їх як єдино вірні без сприйняття сторонньої критики. Зазвичай, сучасні професійні кібершахраї займаючи високі керівні посади в установах та організаціях, володіють спеціальними професійними знаннями та використовують передові технології. Переважна більшість таких осіб має доступ до електронних комунікаційних мереж і відповідних автоматизованих інформаційних систем завдяки своєму службовому статусу. Водночас ці особи небайдужі до пониження власного авторитету або професійного статусу в рамках соціальних груп, в яких працюють.

Аналіз слідчої та судової практики переконливо свідчить про те, що переважна більшість сучасних професійних кібершахраїв вчиняють протиправні діяння шляхом незаконних операцій з використанням ЕОТ, індивідуально, без залучення інших осіб, беручи на себе відповідальність за свої дії. Водночас простежується загрозлива тенденція участі професійних кібершахраїв у групових (організованих) кримінальних правопорушеннях[4].

---

[1] Малій М. І. Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження : дис. на здобуття наук. ступ. доктора філософії. Хмельницький, 2022. С. 175–178.

[2] Брисковська О. М. Соціально-психологічна характеристика особи, яка вчиняє шахрайство в мережі Інтернет. *Науковий вісник Національної академії внутрішніх справ.* Київ: 2020. № 1 (114). С. 75.

[3] Піцик Ю. М. Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету*. 2017. № 26. С. 106.

[4] Швець Д. В. Підходи до визначення психологічного портрета кіберзлочинця. *Актуальні питання*

Важливо визнати, що зовнішня поведінка таких осіб мало відрізняється від соціальних та правових норм, встановлених у суспільстві. До того ж, кібершахраї відзначаються високим професіоналізмом, уважністю та пильністю, а їх дії достатньо витончені, хитромудрі, супроводжуються відмінним маскуванням[1].

Як показують дослідження, проведені Ю. М. Піциком, кримінальні правопорушення, що вчиняються «з використанням високих технологій та кіберпростору, є високоінтелектуальними», а досить великий відсоток осіб, які їх вчиняють, мають дипломи про вищу освіту за фахом «Прикладна інформатика», «Інформаційні системи і технології», «Програмна інженерія», «Інформаційні безпека»[2].

Ми цілком підтримуємо науковців, які відносять зазначені ознаки до визначальних для характеристики сучасних професійних кібершахраїв[3]. Натомість до факультативних ознак цієї категорії правопорушників можна віднести психічні особливості особи, що виявляються в особливому ставленні до ЕОТ та інформаційних технологій, емоційну залежність від них, ескапізм, який О. В. Ткачова, К. В. Науменко[4] та С. М. Лозова[5] визначають як «втечу від дійсності, прагнення піти від реальності, від загальноприйнятих норм суспільного життя у світ ілюзій та псевдодіяльності».

Враховуючи розглянуті вище характеристики сучасних професійних кібершахраїв, варто звернути увагу на те, що дослідники нерідко виділяють так звану «білокомірцеву кримінальну протиправність» (від англ. White-collar crime), яка вирізняється ознакою приналежності зловмисника до числа осіб, які виступають у ролі представників держави, бізнесу, службових осіб і чиновників. Саме Едвіну Сатерленду, відомому американському вченому, ми завдячуємо першим визначенням правопорушень, які позначаються як «білокомірцеві злочини»[6].

Сатерленд заклав основи для дослідження, яким в подальші роки продовжували займатися й інші науковці, поглиблюючи модель «білокомірцевого кримінального правопорушення» та адаптуючи це поняття до конкретних практичних методів та соціально-економічних змін.

протидії злочинності та торгівля людьми : зб. матеріалів Всеукр. наук-прак. конф. (Харків, 23 листоп. 2018 р.). Харків : Харків. нац. ун-т внутр. справ, 2018. С. 120.

[1] Біленчук П. Д., Малій М. І. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття. *Юридичний Вісник України*, 2019, № 40. С. 14–15.

[2] Піцик Ю. М. Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція»*. 2017. № 26. С. 105–107.

[3] Біленчук П. Д., Малій М. І., Харитоненко І. Хакери, фрікери, кіберкрекери… Частина 1. *Юридичний вісник України.* URL: https://lexinform.com.ua/dumka-eksperta/hakery-frikery-kiberkrekery/ (дата звернення: 28.01.2025).

[4] Ткачова О. В., Науменко К. В. Кримінологічна характеристика кіберзлочинця. *Юридичний науковий електронний журнал*. 2018. № 2. С. 200–204.

[5] Лозова С. М. Деякі особливості психічних девіацій кіберзлочинця // Актуальні питання розслідування кіберзлочинів: матеріали міжнарод. наук.-практич. конф.: м. Харків, 10 груд. 2013 р. / МВС України, Харків. нац. ун-т внутріш. справ. Київ: ВАІТЕ, 2013. С. 134–137.

[6] «Білокомірцева злочинність»: таке серйозне звинувачення вимагає захисту високого рівня. *ILA (International Lawyers Associates)* : веб-сайт. URL: https://internationallawyersassociates.com/uk/злочини-білих-комірців (дата звернення: 28.01.2025).

З того моменту, кримінологічні розслідування вже не велися стосовно окремих осіб, а стосовно комплексної та структурованої кримінальної поведінки, залежної від організації економічної діяльності підприємства.

В цьому контексті досліджувала особу кіберзловмисника Л. В. Борисова, яка відмітила, що «у професійно-кваліфікаційному плані коло комп'ютерних злочинців надзвичайно широке: до них відносять різноманітні категорії керівників і спеціалістів – комерційні директори, банківські службовці, фінансисти, програмісти, інженери-наладчики і монтажники комп'ютерного устаткування, бухгалтери тощо»[1].

За даними, які наводять П.Д. Біленчук, М.І. Малій, «52% осіб, які вчиняли шахрайства з використанням ЕОТ, мали спеціальну підготовку в галузі автоматизованої обробки інформації, 97% були службовцями державних установ і організацій, які використовували комп'ютерні системи, мережі та інформаційні технології в своїх виробничих процесах, а 30% мали безпосереднє відношення до експлуатації засобів комп'ютерної техніки». Також зазначені науковці звертають увагу на те, що велику кількість осіб, які вчиняли шахрайства з використанням ЕОТ, (понад 25%) становлять керівники всіх рангів[2]. На думку авторів, крім іншого, це зумовлено тим, що керівник є спеціалістом високого класу, який володіє достатніми професійними знаннями, має безпосередній доступ до широкого кола інформації, може давати відповідні вказівки та розпорядження й безпосередньо юридично не відповідає за роботу комп'ютерної техніки, що дає підстави для їх віднесення до «білокомірцевих злочинців»[3].

Спираючись на дослідження В. В. Пивоварова, можемо виокремити ознаки кримінального професіоналізму сучасного кібершахрая, якими є: 1) відпрацьований тип кримінальної діяльності (спеціалізація); 2) необхідні знання та уміння (кваліфікація); 3) вчинення кримінальних правопорушень для забезпечення засобів до існування (кримінальне ремесло); 4) зв'язок з кримінальним оточенням, здійснюваний через кримінальну спільноту[4].

Аналіз матеріалів кримінальних проваджень, відкритих за ознаками кримінальних правопорушень досліджуваної категорії, здійснений О. А. Самойленко, свідчить про те, що у 20% шахрайств, вчинених у кіберпросторі, місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації знаходилося за межами України, у 40% таких шахрайств здійснювалася підготовка (розробки вірусу, програм зламу, добору паролів) і у10% таких шахрайств використовувався комп'ютер або сервер, які застосовувалися для обробки інформаційного

[1] Борисова Л. В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права*. 2008. Вип. 44. С. 78–79. URL: http://www.apdp.in.ua/v44/15.pdf (дата звернення: 28.01.2025).

[2] Біленчук П. Д., Малій М. І. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? *Юридичний вісник України*, 2019. № 39. С. 14–15.

[3] Там само. С. 14–15.

[4] Пивоваров В. В. До питання співвідношення білокомірцевої та корпоративної злочинності. *Право і суспільство.* 2018. № 1. Ч. 1. С. 223–227.

продукту – предмета посягання[1].

Зарубіжними фахівцями розроблені різноманітні класифікації способів вчинення кібершахрайств, які відповідно кодифікатору Генерального Секретаріату Інтерполу позначаються: QF – комп'ютерне шахрайство; QFC – шахрайство з банкоматами; QFF – комп'ютерна підробка; QFG – шахрайство з ігровими автоматами; QFM – маніпуляції з програмами введення виводу; QFP – шахрайства з платіжними засобами; QFT – телефонне шахрайство; QFZ – інші комп'ютерні шахрайства[2].

Наведені та інші результати наукових досліджень, які проводилися в Україні, Європі та по всьому світу в період від 1998 до 2024 рік, стосовно фактичного стану та видів сучасних професійних кібершахраїв, дають можливість класифікувати їх і розподілити на окремі групи. Виходячи з цього, серед осіб, які сьогодні вчиняють шахрайства, шляхом незаконних операцій з використанням ЕОТ, можна виділити наступні категорії:

1) *скамери* – кібершахраї, які займаються багатьма видами шахрайств, що передбачають заволодіння віртуальними активами шляхом обману людей, які прагнуть інвестувати або придбати криптовалюти. Скам (від англ. scam – шахрайство, афера, обман), це шахрайство, що здійснюється окремою особою або групою людей в бік конкретного користувача, і зазвичай може мати форму або неправдивої обіцянки, або навіть погрози та примусу щось зробити[3]. Як правило, такими засобами користуються скамери у дейтингах (вертикаль в арбітражі трафіку, яка пов'язана із просуванням сервісів, сайтів та додатків для знайомств, за допомогою яких користувачі шукають романтичні або сексуальні стосунки)[4]. До найпоширеніших різновидів скаму належать фішинг/спуфінг, про які мова піде нижче.

2) *фішери* – кібершахраї, які спеціалізуються на фішингу (fishing) – виді кібершахрайства, метою якого є отримання доступу до конфіденційних даних користувачів, логінів, паролів шляхом направлення повідомлення з пропозицією підтвердити дані облікового запису (онлайн-аукціони, лотереї, банківські послуги, інтернет-магазини тощо) з прямим посиланням на сайт, використання на якому особою його логіну та паролю дозволяє отримати доступ до її акаунту, банківського рахунку або персональних даних. Характерною ознакою таких сайтів є їх подібність до загальновідомих інтернет-ресурсів[5]. Фішинг залишається однією з найчастіших форм

[1] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / О.А. Самойленко; за заг. ред. А.Ф. Волобуєва. Одеса: ТЕС, 2020. С. 112.

[2] Комп'ютерне шахрайство. Вікіпедія : веб-сайт. URL: https://uk.wikipedia.org/wiki/Комп%27ютерне_шахрайство (дата звернення 28.01.2025).

[3] Що таке скам? Його види та супутні ризики. *ЦеКрипто* : веб-сайт. URL: https://tsecrypto.com/article/shho-take-skam-jogo-vydy-ta-suputni-ryzyky/ (дата звернення 28.01.2025).

[4] Що таке дейтинг в арбітражі трафіку і як з ним працювати. *Uaff – інноватівний медіа-проект про Арбітраж Трафіку* : веб-сайт. URL: https://uaff.media/blog/shcho-take-deytynh-v-arbitrazhi-trafiku-i-iak-z-nym-pratsiuvaty/ (дата звернення 28.01.2025).

[5] Сучасні інструменти боротьби з кібершахрайствами у банках : монографія / О. В. Кузьменко, Г. М. Яровенко, С. В. Лєонов та ін. ; за заг. ред. О. В. Кузьменко, Г. М. Яровенко. Суми : Видавництво

кібершахрайства. Згідно зі звітом української служби безпеки (СБУ), у 2024 році було зареєстровано понад 5000 випадків фішингу, що на 20% більше у порівнянні з попереднім роком[1];

3) *вішери* (від vishing або голосовий фішинг). Вішинг – варіація фішингу, за якої шахраї зв'язуються з жертвами по телефону, також отримав розповсюдження в останні роки. Зловмисники видають себе за співробітників банків чи представників довірених організацій. Шахраї для вішингових атак застосовують соціальну інженерію. Це особлива техніка, яка ґрунтується на природних інстинктах, властивих людям. До них належить страх, довіра, бажання надати допомогу, жадібність. Завдання зловмисників – пробудити в жертві ці почуття, похитнути її рівновагу, посіявши паніку, або пробудивши інші сильні емоції[2];

4) смішери (від SMiShing – вид фішингу через SMS). Смішинг – це форма фішингу, в якій зловмисник використовує переконливе текстове повідомлення, щоб обманом обдурити цільових одержувачів, щоб вони натиснули на посилання і відправили зловмиснику особисту інформацію або завантажили шкідливі програми на смартфон. Головне завдання смішерів зробити акцент на терміновості. У більшості випадків зловмисники просять виконати необхідну дію негайно: доки гроші з рахунку не пішли, тарифний план автоматично не змінився, банківська картка не заблокувалась назавжди тощо[3];

5) *спуфери* (Spoofers). Спуфінг (spoofing attack) – це практика маніпулювання засобами комунікації, такими як телефонні номери, адреси електронної пошти чи веб-сторінки, щоб вони виглядали правдоподібно та реалістично. Ця техніка часто використовується у атаках фішингу для завоювання довіри жертв. У романтичних аферах спуфінг може використовуватись для надання більшої правдоподібності фальшивим профілям у соціальних мережах або на платформах знайомств[4];

6) *романтичні аферисти* (від Romance Fraud). Романтичні афери, також відомі як любовне шахрайство, є особливо підступною формою кіберзлочину, спрямованої використання емоційних потреб і довіри людей. Зловмисники можуть використовувати «медові пастки» (honeytrap) – це різновид соціальної інженерії, в якому кібершахраї створюють фальшиві профілі у соціальних мережах і на сайтах знайомств з викраденими фото, аби привабити потенційні цілі. В подальшому вони створюють інтимні стосунки з жертвами онлайн і переконують їх переказувати гроші під різними приводами. Національна поліція України повідомила, що у 2024

«Ярославна», 2018. С. 68–71.

[1] Огляд на шахрайство та інтернет-афери в Україні. *Німецький центр Аренс і Шварц* : веб-сайт. URL: https://ahrens.kiev.uaОгляд-шахрайство-інтернет-афери-Україні-496-ua.html (дата звернення 28.01.2025).

[2] Телефонне шахрайство вішинг – що це таке і як з ним боротися? *MFO-Ukraine.com*: веб-сайт. URL: https://www.mfo-ukraine.com/2023/01/vishing.html (дата звернення 28.01.2025).

[3] Кібершахрайство: Фішинг. Вішинг. Смішинг. Бейтінг. *Правничий дім «Копірайт»* : веб-сайт. URL: https://kopirait.com.ua/kibershahrajstvo-fishyng-vishyng-smishyng-bejting/ (дата звернення 28.01.2025).

[4] Там само.

році понад 1500 людей в Україні стали жертвами романтичних афер, при цьому загальна шкода оцінюється у понад 12 мільйонів доларів США[1]. Це число красномовно показує, що такий вид шахрайства особливо поширений в Україні і є тривожна тенденція до зростання. Цей факт наголошує на серйозній загрозі цього виду шахрайства, особливо в умовах розвитку платформ для знайомств;

7) *шахраї в бізнес-електронній пошті (business e-mail compromise, BEC)*. Компрометація корпоративної електронної пошти – це просунутий вид кібератак, націлений на підприємства та організації. До прикладу, він може включати обман співробітника або керівника для виконання грошового переказу, або ж злам електронної пошти працівника чи управлінця для відправки листів зі шкідливим кодом контактам компанії (клієнтам, постачальникам тощо). Кримінальна діяльність шахраїв BEC спрямована на завдання збитків компаніям, при цьому зловмисники видають себе за керівників або партнерські компанії та ініціюють переказ великих грошей на свої рахунки. За даними Міністерства економіки України, минулого року було зареєстровано понад 300 випадків шахрайства BEC, із загальним збитком близько 9 мільйонів доларів США[2];

8) *бейтери*. Бейтинг – це тип атаки із використанням соціальної інженерії, під час якої зловмисники спонукають користувача надати свої конфіденційні дані, обіцяючи щось в обмін (наприклад, безкоштовне завантаження ігор, музики чи фільмів). Бейтинг може набувати і матеріальної форми: наприклад, шахраї можуть залишити USB-накопичувач або жорсткий диск із шкідливим програмним забезпеченням та загадковим написом, наприклад, «План звільнення Q1», у громадському місці і почекати, поки хто-небудь цікавий не забере їх і не спробує з'ясувати, що на них знаходиться. Щойно людина підключить флешку або диск до комп'ютера, хакерська програма активується автоматично і завантажить шкідливий файл на комп'ютер жертви, що дає змогу зловмиснику заволодіти доступом до потрібних технічних засобів та інформації[3];

9) *кардери* (carders) – кібершахраї, які здійснюють дії з пластиковою карткою іншої людини без дозволу з його боку. Кардінг (carding) – це вид шахрайства, при якому відбувається платіжна операція з використанням картки або реквізитів, яка не була ініційована власником картки, або не була їм підтверджена. Кардери збирають інформацію про картки обманним шляхом, вони викрадають не тільки номери карток, ініціали власників та термін дії, але і добираються до PIN та CVV-кодів.[4].

---

[1] Огляд на шахрайство та інтернет-афери в Україні. *Німецький центр Аренс і Шварц* : веб-сайт. URL: https://ahrens.kiev.uaОгляд-шахрайство-інтернет-афери-Україні-496-ua.html (дата звернення 28.01.2025)

[2] Огляд на шахрайство та інтернет-афери в Україні. *Німецький центр Аренс і Шварц* : веб-сайт. URL: https://ahrens.kiev.uaОгляд-шахрайство-інтернет-афери-Україні-496-ua.html (дата звернення 28.01.2025)

[3] Кібершахрайство: Фішинг. Вішинг. Смішинг. Бейтінг. *Правничий дім «Копірайт»* : веб-сайт. URL: https://kopirait.com.ua/kibershahrajstvo-fishyng-vishyng-smishyng-bejting/ (дата звернення 28.01.2025).

[4] Омельяненко М. особливості криміналістичної характеристики Інтернет-шахрайства.

Варто зауважити, що кількість категорій кібершахраїв не обмежується лише наведеними у цій класифікації. Їх стає дедалі більше і вони постійно розвиваються і спотворюються, переростаючи у більш складні форми кібершахрайства в залежності від способів вчинення.

Підсумовуючи зазначене, можна сформувати сучасний портрет типового професійного кібершахрая: це особа чоловічої статі, віком 22–42 роки, офіційно неодружена (розлучена або перебуває у вільних стосунках), не має судимостей, має вищу (технічну) освіту, амбіційна, інтелектуально розвинута, ввічлива, артистична, творча, «інтроверт» за складом характеру, є експертом у галузі кібербезпеки, володіє глибокими фаховими знаннями в області інформаційної безпеки, включаючи програмування, аналіз даних, криптографію та управління ризиками. Може працювати в різних сферах, включаючи ІТ-компанії, урядові установи, фінансові організації та приватний сектор. Відмітними рисами сучасного професійного портрету кібершахрая слід вважати: схильність до авантюризму, імперсоналізація (здатність видавати себе за іншу особу для отримання вигоди), рішучість, виваженість, толерантність, пильність, витримка, зосередженість, системність, дисциплінованість, емпатійність (уміння поставити себе на місце жертви, здатність відчувати її внутрішній світ і психічний стан), здатність до передчуття, творче мислення, авторитетність, вміння виявляти вразливості жертви та підбирати способи маніпуляції і впливу на неї.

Висновки. Використання запропонованої типології сучасного портрету професійного кібершахрая, дає можливість визначення соціально-психологічних даних про особу відповідно до ознак шахрайства, вчиненого ним шляхом незаконних операцій з використанням ЕОТ, окреслити ефективні шляхи його викриття, оптимізувати процес виявлення кола осіб, серед яких слід вести оперативний пошук правопорушника. Запропоновані особливості сучасного портрету професійного кібершахрая є також підґрунтям для вдосконалення методики розслідування кримінальних правопорушень досліджуваної категорії, визначення тактики проведення слідчих (розшукових) та негласних слідчих (розшукових) дій, застосування оперативно-розшукових можливостей, зокрема, використання конфіденційного співробітництва під час здійснення оперативного супроводження кримінального провадження, організації заходів протидії та превенції шахрайств, вчинених шляхом незаконних операцій з використанням ЕОТ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Білокомірцева злочинність»: таке серйозне звинувачення вимагає захисту високого рівня. ILA (International Lawyers Associates) : вебсайт. URL: https://internationallawyersassociates.com/uk/злочини-білих-комірців (дата звернення: 28.01.2025).

URL: http://kpk.org.ua/2007/12/18/osobennosti-kriminalisticheskojj.html (дата звернення 28.01.2025).

2. Біленчук П. Д., Малій М. І. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? *Юридичний вісник України*, 2019. № 39. С. 14–15.

3. Біленчук П. Д., Малій М. І. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття. *Юридичний Вісник України*, 2019, № 40. С. 14–15.

4. Біленчук П. Д., Малій М. І. Пріоритетні напрями досліджень психологічного портрету електронного зловмисника. *Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів*: зб. тез Міжнар. наук.-практ. конф. (м. Київ, 30 жовтня 2020 р.). Київ : ДНДІ МВС України, 2020. С. 79–81.

5. Біленчук П., Малій М., Харитоненко І. Хакери, фрікери, кіберкрекери… Частина 1. *Юридичний вісник України.* URL: https://lexinform.com.ua/dumka-eksperta/hakery-frikery-kiberkrekery/ (дата звернення: 28.01.2025).

6. Борисова Л. В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права*. 2008. Вип. 44. С. 76–81. URL: http://www.apdp.in.ua/v44/15.pdf (дата звернення: 28.01.2025).

7. Брисковська О. М. Соціально-психологічна характеристика особи, яка вчиняє шахрайство в мережі Інтернет. *Науковий вісник Національної академії внутрішніх справ.* 2020. № 1 (114). С. 70–78.

8. Кібершахрайство : Фішинг. Вішинг. Смішинг. Бейтінг. *Правничий дім «Копірайт»* : веб-сайт. URL: https://kopirait.com.ua/kibershahrajstvo-fishyng-vishyng-smishyng-bejting/ (дата звернення 28.01.2025).

9. Комп'ютерне шахрайство. Вікіпедія : веб-сайт. URL: https://uk.wikipedia.org/ wiki/Комп%27ютерне_шахрайство (дата звернення 28.01.2025 р.).

10. Лозова С. М. Деякі особливості психічних девіацій кіберзлочинця // Актуальні питання розслідування кіберзлочинів: матеріали міжнарод. наук.-практич. конф.: м. Харків, 10 груд. 2013 р. / МВС України, Харків. нац. ун-т внутріш. справ. Київ: ВАІТЕ, 2013. С. 134–137.

11. Малій М. І. Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження : дис. на здобуття наук. ступ. доктора філософії. Хмельницький, 2022. 224 с.

12. Огляд на шахрайство та інтернет-афери в Україні. *Німецький центр Аренс і Шварц* : веб-сайт. URL: https://ahrens.kiev.uaОгляд-шахрайство-інтернет-афери-Україні-496-ua.html (дата звернення 28.01.2025).

13. Омельяненко М. особливості криміналістичної характеристики Інтернет-шахрайства. URL: http://kpk.org.ua/2007/12/18/osobennosti-kriminalisticheskojj.html (дата звернення 28.01.2025).

14. Пивоваров В. В. До питання співвідношення білокомірцевої та корпоративної злочинності. *Право і суспільство*. 2018. № 1. Ч. 1. С. 223–227.

15. Піцик Ю. М. Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету*. Серія «Юриспруденція». 2017. № 26. С. 105–107.

16. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / За заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

17. Сучасні інструменти боротьби з кібершахрайствами у банках : Монографія / О. В. Кузьменко, Г.М. Яровенко, С. В. Лєонов та ін. ; за заг. ред. О. В. Кузьменко, Г. М. Яровенко. Суми : Видавництво «Ярославна», 2018. 144 с.

18. Телефонне шахрайство вішинг – що це таке і як з ним боротися? *MFO-Ukraine.com*: веб-сайт. URL: https://www.mfo-ukraine.com/2023/01/vishing.html (дата звернення 28.01.2025).

19. Ткачова О. В., Науменко К. В. Кримінологічна характеристика кіберзлочинця. *Юридичний науковий електронний журнал*. 2018. № 2. С. 200–204.

20. Швець Д. В. Підходи до визначення психологічного портрета кіберзлочинця. *Актуальні питання протидії злочинності та торгівля людьми* : зб. матеріалів Всеукр. наук-прак. конф. (Харків, 23 листоп. 2018 р.). Харків : Харків. нац. ун-т внутр. справ, 2018. С. 118–121.

21. Що таке дейтинг в арбітражі трафіку і як з ним працювати. *Uaff – інноватівний медіа-проект про Арбітраж Трафіку* : веб-сайт. URL: https://uaff.media/blog/shcho-take-deytynh-v-arbitrazhi-trafiku-i-iak-z-nym-pratsiuvaty/ (дата звернення 28.01.2025).

22. Що таке скам? Його види та супутні ризики. *ЦеКрипто* : веб-сайт. URL: https://tsecrypto.com/article/shho-take-skam-jogo-vydy-ta-suputni-ryzyky/ (дата звернення 28.01.2025).

Стаття надійшла до редакції 30.01.2025

Olersii Ol. DEREVIAHIN,
Phd in Law, Senior Researcher
(Kharkiv National University of Internal Affairs, Kharkiv, Ukraine)

Dmytro V. PASHNIEV,
Phd in Law, Associate Professor
(Kharkiv National University of Internal Affairs, Kharkiv, Ukraine)

Anton Ol. NOVYTSKYI,
PhD in Law
(Main Department of the National Police of Ukraine, Kharkiv, Ukraine)

SPECIFIC APPROACHES TO DEFINING THE MODERN PORTRAIT OF A PROFESSIONAL CYBERFRAUD

Based on the analysis of the works of domestic and foreign scientists dedicated to the criminological, forensic, and socio-psychological characteristics of individuals who have committed cyber fraud, the article proposes to determine the typologies of the modern portrait of a professional cyber fraudster according to the type of fraud committed through illegal operations using computer technology that allows to secure the life activities of individuals, citizens, local government institutions, state authorities, and the global society from criminal violations in cyberspace.

The proposed features of the modern profile of a professional cyber fraudster serve as a basis for improving the methodology of investigating criminal offenses in the studied category, determining the tactics of investigative (search) and covert investigative (search) actions, applying operational and investigative capabilities, including the use of confidential cooperation during the operational support of criminal proceedings, organizing measures to counter and prevent fraud committed through illegal operations using electronic computing technology.

Key words: *cyber fraud, cyber fraudster, typology, illegal operations, computer technology.*