

УДК: 343.98

ORCID: 0000-0003-1861-8354

e-mail: gull_ukr@ukr.net

Larysa P. Grynko,
Associated Professor at the Department
of Criminal Law and Criminal Law
Disciplines (Poltava Law Institute of
The Yaroslav Mudryi National Law
University)

Гринько Лариса Петрівна,
доцент кафедри кримінального права
та кримінально-правових дисциплін
(Полтавський юридичний інститут
Національного юридичного
університету імені Ярослава Мудрого)

**ОСОБА ЗЛОЧИНЦЯ ЯК ЕЛЕМЕНТ
КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ
ШАХРАЙСТВ, УЧИНЕНИХ З ВИКОРИСТАННЯМ МЕРЕЖІ
ІНТЕРНЕТ**

**THE PERSON OF THE CRIMINAL AS AN ELEMENT OF
CRIMINAL CHARACTERISTICS OF SCAMS COMMITTED
USING THE INTERNET**

Анотація. У статті надано характеристику особи злочинця при вчиненні шахрайства з використанням мережі Інтернет. Проаналізовано судову практику та позицій вчених-криміналістів з окресленої проблематики. Встановлено, що на сьогодні простежується тенденція до збільшення злочинів, які вчинюються в мережі Інтернет або якимось з нею пов'язані. Стрімке використання ІТ-технологій зумовлює постійне виникнення нових шахрайських схем, удосконалення вже існуючих. Як наслідок, суттєво зростає складність виявлення і розслідування злочинів цих категорій. Дослідження особи злочинця постає центральною ланкою криміналістичної характеристики досліджуваного злочину, оскільки від рівня дослідження такого структурного елемента, його поведінки, залежить ефективність розкриття та розслідування цього злочину.

Надано криміналістичну характеристику особі-шахрая, досліджено окремі категорії Інтернет-шахраїв. Особа-шахрая – це особа, яка має відчуття переваги та презирливе ставлення до інших, необхідний інтелектуальний рівень, у неї розвинені комунікативні риси, винахідливість, відчуває себе впевнено та користується довірливістю людей. Для неї характерні відсутність жалю, моральних принципів. Здійснено спробу його класифікації на три групи шахраїв, які вчинюють шахрайства в мережі Інтернет: одноособово; у співучасті; у складі організованої злочинної групи. До першої та другої групи можна віднести осіб, які, як правило, створюють сторінку з продажу речей або сайти купівлі/продажу товарів, сайтів-двійників, використовують втрачені чи викрадені картки тощо. Для них не принципові знання у сфері ІТ-технологій. Для третьої групи характерний не тільки розподіл ролей, а й рівень професійної підготовки учасників організованої злочинної групи. Ці види шахрайств є більш небезпечними злочинами, вони носять тривалий характер і не обмежуються одним епізодом. За наслідками вчинений злочин є більш тяжким, його скоюють в особливо великих розмірах.

Ключові слова: шахрайство, комп'ютерні технології, шахрайство в мережі Інтернет, кіберзлочини, особа злочинця, інтернет-шахрай, особа потерпілого.

Summary. The article describes the identity of the offender in committing fraud using the Internet. Judicial practice and positions of criminologists on the outlined issues are analyzed. There is an increase in crimes committed on the Internet or in connection with it. This situation is a trend. The constant use of IT technologies leads to the constant emergence of new fraudulent schemes, the improvement of existing ones. As a result, the complexity of detecting and investigating crimes is growing significantly. Investigation of the identity of the offender is a central element of the forensic characterization of fraud. The effectiveness of the detection and investigation

of Internet fraud depends on the level of research into the identity of the offender, his behavior.

Investigated the forensic characterization of the person-swindler is given, separate categories of Internet swindlers. A swindler is a person who has a sense of superiority and contempt for others, the necessary intellectual level, he has developed communication skills, ingenuity, feels confident and enjoys the trust of people. It is characterized by a lack of pity, moral principles. An attempt was made to classify it into three groups of fraudsters who commit fraud on the Internet: one-person; in complicity; as part of an organized criminal group. The first and second groups include people who usually create a page for selling things or sites for buying / selling goods, duplicate sites, use lost or stolen cards, and so on. They do not have basic knowledge in the field of IT technologies. The third group is characterized not only by the distribution of roles, but also the level of professional training of members of an organized criminal group. These types of fraud are more dangerous crimes, they are long-lasting and not limited to one episode. As a result, the crime is more serious, it is committed on a particularly large scale.

Keywords: fraud, computer technology, Internet fraud, cybercrime, the identity of the offender, Internet fraud, the identity of the victim.

Постановка проблеми. Розвиток інформаційних технологій, впровадження їх у всі сфери життєдіяльності людини розширює не лише можливості для суспільних відносин, а й створює умови для вчинення різноманітних злочинів, пов'язаних з заволодінням чужим майном. Безперечно, сьогодні важливе місце займають інтернет ресурси, тому все більше злочинів вчинюються саме через мережу Інтернет.

Шахрайство в мережі Інтернет є одним з найрозповсюджених способів незаконного заволодіння чужим майном. Найчастіше шахраї створюють сайти і продають неіснуючий товар, виманюють інформацію з карток, має місце онлайн-кредитування тощо. Лише за минулий рік в Україні сталося майже 72

тисячі випадків незаконних дій із платіжними картами, 58% із них – в Інтернеті. Так, у першому півріччі минулого року банки повідомили про фіксацію 47,5 тис. випадків шахрайства з картками на загальну суму 86,4 млн грн, тоді як за перше півріччя 2019 року було зафіксовано 34,7 тис. випадків на 72,6 млн грн. Тобто відбулося зростання обсягів шахрайств [1].

Стан опрацювання обраної проблематики, аналіз останніх публікацій та досліджень. Дослідженню шахрайства через мережу Інтернет присвятили свої наукові праці А. І. Анапольська, Р. С. Атаманов, С. В. Головкін, С. М. Князєв, Н. Ю. Кириленко, Н.С. Карпов, С. М. Князєв, А. В. Крижевський, О. В. Курман, О. Л. Мусієнко, Т. В. Охрімчук, Т. А. Пазинич, В. П. Сабадаш, С.В. Самойлов, М. М. Федотов, С. С. Чернявський та інші. Ці вчені-криміналісти внесли вагомий внесок в у розробку методичних рекомендацій з розслідування цього виду злочину. Разом з тим, ця сфера дослідження не втрачає своєї актуальності, оскільки поява нових схем вчинення шахрайств з використанням мережі Інтернет потребує дослідження всіх його структурних елементів і, насамперед, особи, яка його скоїла. Тому дослідження особи злочинця є одним з актуальних питань, яке постає сьогодні під час розкриття та розслідування шахрайств, вчинених з використанням мережі Інтернет.

Метою статті є дослідження особи злочинця як елемента криміналістичної характеристики вчинення шахрайств з використанням мережі Інтернет, визначення його особливостей, розкриття змісту та надання класифікації.

Виклад основного матеріалу. Особа злочинця є центральним елементом криміналістичної характеристики шахрайств, оскільки вибір способу вчинення злочину, наявність слідової картини завжди пов'язано з особою-шахрая.

У науковій літературі висловлюються різноманітні точки зору стосовно визначення сутності особи злочинця як елемента криміналістичної характеристики кримінальних правопорушень. Особа злочинця – це поняття широке, містить опис людини як соціально-біологічної системи, властивості та

ознаки якої відображаються в матеріальному середовищі та використовуються для розкриття і розслідування злочину, пошуку злочинця, його ідентифікації та викриття у вчиненому злочині [2, с. 345].

Характеристику особи злочинця становлять ті дані, за якими можна визначати ефективні шляхи розшуку та викриття злочинця [3, с.72-73]. Як зазначає М.Т. Ведерніков, у розробці криміналістичної характеристики особи злочинця занадто важко виділити інформацію, що має чисто криміналістичне значення, оскільки особистість – єдине цілісне явище, всі сторони якого взаємозалежні й взаємозумовлені, хоча в науковому відношенні правомірно порушувати питання про криміналістично значущі властивості особи злочинця, криміналістичний аспект у вивченні особи обвинуваченого [4, с. 76]. Це і соціально-демографічні, морально-психологічні, кримінально-правові дані. Значення мають такі відомості про особу злочинця як вік, стать, рід занять, характер злочинної групи наявність взаємин із жертвою злочину тощо.

Аналіз судової практики свідчить, що найчастіше шахрайство в мережі Інтернет вчиняють особи чоловічої статі – 92%, переважно з середньою та вищою освітою – 81%, не працюючі – 76%, раніше судимі – 7%. Що стосується взаємин особи злочинця та особи потерпілого, то у більшості випадків вони не знайомі (складає 94%).

Певний інтерес становлять особливості вікових характеристик розгляданого типу злочинців. Вік осіб, що вчиняють шахрайства в мережі Інтернет, у більшості випадків становить від 25 до 45 років (69%).

Особа-шахрая характеризується високим рівнем інтелектуального розвитку, легко встановлює психологічний контакт, розвинені комунікативні риси, винахідливість, входить у довіру до інших людей. Як зазначає В.Ю. Шепітько, особа-шахрая характеризується специфічним комплексом ознак. Більшість злочинців мають сильний дар уяви, вони використовують вплив і вміння переконувати людей [5, с. 144]. Крім того, як вважає Карчевський М. В., шахраї – це висококваліфіковані професіонали, що володіють широким

кругозором і знаннями в сфері права, для нього характерне виховання або розвиток вміння імпровізувати, оперативно реагувати на швидко мінливу обстановку [6, с. 47].

Характерним для шахрайств, учинених з використанням мережі Інтернет є те, що особа злочинець особисто не контактує із своєю жертвою. Для особи Інтернет-шахрая притаманні відчуття переваги та презирливе ставлення до інших. Для неї характерні відсутність жалю, моральних принципів. Л. Прудка наголошує, що під час учинення шахрайства для досягнення поставленої мети злочинець намагається застосовувати психологічний вплив на особу за допомогою маніпулювання. До основних прийомів злочинного маніпулювання належать такі: маніпулювання змістом і формою надання інформації, штучне створення браку часу в прийнятті рішення (вимагання сплатити за послугу або товар у якомога стислий строк тощо) [7, с. 144]. Таким прикладом є відкрите кримінальне провадження, де жінка, натрапивши на сайт «Абсолют Глобал Маркет», представники якого пропонували безпечний заробіток з купівлі-продажу товарів або отримання відсотків з грошових вкладів, зробила перший внесок у розмірі 250 доларів за активацію. Також, жінка відправила в «особистий кабінет» всі реквізити особистої кредитної карти. Цього також вимагали «персональні консультанти». Вже наступного дня у потерпілої, начебто, з'явилися клієнти. З нею знову зв'язалися працівники «біржі». Цього разу необхідно було внести вже 1200 доларів для проведення даної угоди. Прибуток обіцяв бути високий, тому жінка зробила все, що від неї вимагалось. Через деякий час знову необхідно було зробити внесок на суму 32 000 гривень. І ось, найбажаніший прибуток в сумі 8 000 доларів! Але щоб його перерахувати необхідно внести ще 2 000 доларів, аби вивести їх на рахунок потерпілої. Цього разу жінка вирішила позичити гроші у своєї доньки, яка і «відкрила очі» матері на те, що відбувається. Таким чином мешканка Волноваха протягом 2 місяців власноруч віддала аферистам загалом майже 130 000 гривень [8].

Характерним для шахрайств в мережі Інтернет є ще й те, що шахраї крім психологічних якостей, мають навички використання комп'ютерних технологій, орієнтуються в використанні банківських карток, обізнані в платіжних системах тощо. О.В. Волобуєв поділяє шахраїв, які володіють навичкам використання комп'ютерної техніки та інших електронних засобів: а) аматори, тобто ті, що діють самостійно, в домашніх умовах і вільний від роботи час, б) високоосвічені спеціалісти, які діють у складі організованих злочинних груп. До другої групи вчений відносить працівників банківських закладів, різноманітних комерційних структур, обчислювальних центрів банківських установ, а також інші потрібні за своїми службовим станом і повноваженнями особи. Необхідно підкреслити, що до складу такої групи обов'язково входить один або кілька учасників, які є програмістами або хоча б володіють знаннями та навичками в галузі комп'ютерних інформаційних технологій [9, с. 181].

У криміналістичній літературі наявні й інші класифікації шахраїв, які діють в мережі Інтернет. Так, М. І. Омеляненко та О. А. Севідов виділяють шахраїв залежно від їх «спеціальності» на такі види: 1) кардери; 2) кіберкруки; 3) фішери; 4) спамери; 5) кіберсквотери; 6) фрікери. Кожному з зазначених видів автори надають характеристику [10, с. 85-86]. Така класифікація заслуговує увагу, оскільки дійсно наявний прямий зв'язок особи злочинця з його навичками та реалізація їх у злочинну діяльність. Разом з тим, запропонована класифікація не є вичерпною, оскільки способи вчинення шахрайств з використанням мережі Інтернет та осіб, які їх вчинюють, набагато більше, ніж окреслено авторами.

Як вбачається, найбільш доцільним є поділ шахраїв на три групи:

- 1) ті, що вчинюють шахрайства в мережі Інтернет одноособово;
- 2) ті, що вчинюють шахрайство у співучасті;
- 3) ті, що вчинюють шахрайство у складі організованої злочинної групи.

До першої та другої групи можна віднести як аматорів, так і «хакерів», які здійснюють свою злочинну діяльність одноособово або у співучасті. Це, як правило, особи, які створюють сторінку з продажу речей або сайти

купівлі/продажу товарів, сайтів-двійників, використовують втрачені чи викрадені картки тощо. Як вважає П. Біленчук, визначальною характеристикою інтернет-шахрая є те, що для вчинення цих злочинів не потрібна спеціальна освіта у сфері комп'ютерних технологій, діапазон рівня спеціальної освіти правопорушників теж широкий – від осіб, які володіють, мінімальними знаннями користувача, до висококваліфікованих фахівців. Крім того, 52 % злочинців мають спеціальну підготовку в галузі автоматизованої обробки інформації, 97 % – були службовцями державних установ та організацій, які використовували комп'ютерні системи й інформаційні технології, а 30 % з них брали участь в експлуатації засобів комп'ютерної техніки. З дослідницької позиції цікавим є факт, що з кожної тисячі комп'ютерних злочинів лише сім учинили професійні програмісти. У деяких випадках особи, які вчинили комп'ютерні злочини, не мали технічного досвіду [11].

Шахрайства, що вчиняються організованою злочинною групою, є більш небезпечними злочинами, вони носять тривалий характер і не обмежуються одним епізодом. За наслідками вчинені злочини є більш тяжкими, злочини скоюють в особливо великих розмірах. Рівню професійної підготовки співучасників приділяється значна увага. В таку злочинну групу входять фахівці у сфері ІТ, психології, економіки, права. У більшості випадків мова йде про створення фіктивний брокерських сайтів чи товарних бірж. На їх частку припадає в середньому 79 % шахрайств, учинених організованими групами. Функції учасників таких компаній чітко визначені. Зловмисники використовують психологічні методи агітаційного характеру з метою інвестування коштів в акції відомих компаній, що котируються на міжнародних фондових біржах. Суть цієї злочинної діяльності зводиться в імітуванні роботи на фондовому ринку з метою привласнення коштів інвесторів, де останні з метою збереження та примноження власних заощаджень нерідко не міркують про те, що можуть потрапити у руки шахраїв. Прикладом є компанія ВІНК – представник надійного брокера, яка пропонує свої фінансові послуги. Так,

громадянину зателефонували з цієї компанії і запропонували відкрити особистий кабінет, завести кошти та грати на коливаннях валют «євро – долар». *Перший рахунок був на 3 тисячі доларів. Але одразу пішов у мінус. Потім ще два рахунки на 4,5 тисячі та на 14,5.* Спочатку була торгівля з роботом, але робот почав давати мінуси. Після цього *залучили нібито дуже досвідченого трейдера, з величезним досвідом, 15 років. Показували прекрасні звіти – як торгує, які хороші результати робить.* Коли мінус обнулив рахунок у всьому звинуватили інвестора. Після цього зник доступ до рахунку, пароль змінився без його відома. Потерпілий втратив 24 000 доларів. Телефон брокера перестав відповідати [12].

І таких прикладів безліч. Головна мета таких шахраїв – під психологічним тиском виманити всі кошти, які є у особи. При цьому такі компанії достатньо часто уникають кримінальної відповідальності, оскільки доказати вину і притягнути до відповідальності таких шахраїв достатньо важко. Реальні кількості ошуканих громадян і обсяги їх коштів залишається невідомою, що дозволяє виділити цю проблему достатньо загрозливою.

І.В. Моргачов серед причин, чому таке явище набуло масового явища, виділяє наступні: - юридична безкарність, як правило відповідні особи є нерезидентами країни та працюють із-за кордону дистанційно; - наявність економічної спокуси, коли шахрайство є безкарним, більшості умовно-брокерським організаціям на «Forex» (в тому числі з торгівлі CFD-контрактами) не вигідно працювати за чесними правилами; - наявність високотехнологічних та витончених схем шахрайства, які разом з використанням здобутків сучасної ІТ-індустрії дозволяють впевнити клієнта, що він сам винен у власному програшу; - неминучий програш людині пояснюють його недосвідченістю, недостатньою сумою на депозиті, невірною стратегією або звичайним невезінням; людину запевняють, що всі ці причини тимчасові, тому треба проходити платні курси, а трейдінг слід продовжити до появи прибутку; - важкість для пересічного громадянина відрізнити добросовісного брокера від шахрая; - наявність високого рівня інвестиційної схильності у громадян та

бажання використання здобутків прогресу: бути трейдером, акціонером, інвестором, бажання зберегти власні заощадження та, навіть, примножити їх; - безкарність умисно брехливої реклами; - недоступність, відсутність або дефіцит об'єктивної інформації щодо імовірності програшу; - відсутність державних та регіональних інституцій, які консультують, обмежують рекламу, блокують відповідні Інтернет-ресурси; - з правової точки зору більшість спорів між клієнтами та умовно-брокерськими організаціями (в тому числі з торгівлі CFD-контрактами) не мають кримінальної ознаки, а мають вирішуватися в судовому порядку як господарські справи; - проблематичність однозначного визначення умовно-брокерських організацій на «Forex» (в тому числі з торгівлі CFD-контрактами) в якості шахрайських для державних органів влади. Як правило ошукані не звертаються до правоохоронних органів, оскільки відповідні схеми є ідеально витонченими і високотехнологічними, що не дозволяє довести злочин та притягнути шахрая до кримінальної та адміністративної відповідальності [13, С. 76-77].

Висновки та пропозиції. У підсумку зазначимо, що на сьогодні чітко простежується збільшення злочинів, що вчинюється в мережі Інтернет. Стрімке використання ІТ-технологій зумовлює виникнення нових шахрайських схем. Як наслідок, суттєво зростає складність виявлення і розслідування цих злочинів. Тому, дослідження особи злочинця постає центральною ланкою криміналістичної характеристики досліджуваного злочину, оскільки від рівня дослідження такого структурного елемента, його поведінки, залежить ефективність розкриття та розслідування цього злочину.

Література

1. Марчук В. Карткове шахрайство: нові «мутації» старих схем. Укрінформ. URL: <https://www.ukrinform.ua/rubric-economy/3230485-kartkove-sahrajstvo-novi-mutacii-starih-shem.html>. (дата звернення до ресурсу: 27.11.2021).

2. Шеремет А.П. Криміналістика: навчальний посібник. Київ: Центр учбової літератури, 2005. 472 с.
3. Антонова Н. О., Рибачук Л.І. Психологічна зрілість як основа готовності до професійної діяльності психолога. URL: <http://journals.urau.ua/index.php/2227-6246/article/view/162200>. (дата звернення до ресурсу: 27.11.2021).
4. Ведерников Н.Т. Личность преступника как элемент криминалистической характеристики преступления. *Криминалистическая характеристика преступлений: сб. науч. тр.* 1985. С. 76-79.
5. Шепітько В. Ю. Особливості криміналістичної характеристики шахрайства. *Вісник Академії правових наук України*. 1998. № 2. С. 144-150.
6. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України. Луганськ: РВВ ЛДУВС, 2012. 327 с.
7. Прудка Л. М. Психологічні особливості шахрайства в мережі Інтернет. *Південноукраїнський правничий часопис*. 2018. № 2. С. 30-33. URL: <http://www.sulj.oduvs.od.ua/archive/2018/2/10.pdf>. (дата звернення до ресурсу: 27.11.2021).
8. Поліція Волновахи відкрила кримінальне провадження за фактом шахрайства на суму в майже 130 000 гривень. Волноваський районний відділ поліції. URL: <http://www.volnovaha-police.dn.ua/news/view/3923>. (дата звернення до ресурсу: 27.11.2021).
9. Волобуєв А.Ф. Особливості розслідування розкрадань грошових коштів, що здійснюються з використанням комп'ютерної техніки. *Вісник Луганського інституту внутрішніх справ МВС України*. 1998. № 2. С. 179-185.
10. Омеляненко М. Особенности криминалистической характеристики Интернет-мошенничества. URL: <http://kpk.org.ua/2007/12/18/osobennosti-kriminalisticheskoyj.html>. (дата звернення до ресурсу: 27.11.2021).

11. Біленчук П.Д. Питання соціальної та криміналістичної характеристики комп'ютерного злочинця. URL: <http://www.crime-research.ru/library/Bilen3.htm>. (дата звернення до ресурсу: 27.11.2021).

12. Іваницький О. Брокери-шахраї. Як «молоді й успішні» розводять українців на гроші. Інформаційне агенство УНІАН. 29 березня 2021 року. URL: <https://www.unian.ua/society/brokeri-shahraji-yak-molodi-y-uspishni-rozvodyat-ukrajinciv-na-groshi-novini-ukrajini-11370178.html>. (дата звернення до ресурсу: 27.11.2021).

13. Моргачов І.В. Протидія шахрайству на регіональних фінансових ринках. *Вісник Хмельницького національного університету*. 2019. № 1. С. 76-78. URL: <http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/17-14.pdf>. (дата звернення до ресурсу: 27.11.2021).