УДК 343.91:343.72 doi: https://doi.org/10.33270/01201141.70

Брисковська О. М. – кандидат юридичних наук, старший науковий співробітник, провідний науковий співробітник наукової лабораторії з проблем протидії злочинності навчально-наукового інституту № 1 Національної академії внутрішніх справ, м. Київ
ORCID: https://orcid.org/0000-0001-6902-9969

Соціально-психологічна характеристика особи, яка вчиняє шахрайство в мережі Інтернет

Мета *статті – встановити особливості соціально-психологічного портрета особи, яка вчиняє шахрайства в мережі Інтернет, на підставі аналізу науково-теоретичних поглядів і результатів дослідження вітчизняних та іноземних учених щодо соціально-психологічної характеристики шахрая та особи, яка вчиняє злочини в мережі Інтернет.* ***Методологія.*** *У науковій статті використано цілісну й узгоджену систему методів, що дала змогу проаналізувати предмет дослідження, зокрема застосовано методи аналізу, індукції та дедукції. Теоретичним підґрунтям публікації стали праці вітчизняних й іноземних учених, присвячені психологічним, соціальним, соціально-психологічним характеристикам осіб, які вчиняли шахрайства та злочини в мережі Інтернет.* ***Наукова новизна*** *полягає в узагальненні соціально-психологічної характеристики особи, яка вчиняє шахрайства в мережі Інтернет. Це дає змогу визначити соціально-психологічний портрет злочинця відповідно до виду вчиненого інтернет-шахрайства, що підвищить ефективність розслідування таких злочинів.* ***Висновки.*** *Встановлено соціально-психологічні риси, притаманні інтернет-шахраям, що має спростити процес виявлення злочинця у віртуальному світі. Узагальнена соціально-психологічна характеристика особи інтернет-шахрая надасть можливість скласти соціально-психологічний портрет за вчиненим інтернет-шахрайством й обрати ефективні шляхи його викриття, оптимізувати процес виявлення кола осіб, серед яких слід шукати злочинця, і визначити правопорушника. Окреслені риси портрета інтернет-шахрая становлять підґрунтя для розслідування злочину й організації заходів протидії та профілактики шахрайств, учинених за допомогою мережі Інтернет. У статті обґрунтовано важливе значення складання типового соціально-психологічного портрета інтернет-шахрая. Соціально-психологічна характеристика поведінки особи, яка вчиняє шахрайства в мережі Інтернет, сприятиме вдосконаленню методів розслідування та своєчасній ідентифікації таких виявів.*

Ключові слова: Інтернет; інтернет-шахрайство; кіберзлочинець; інтернет-шахрай; особа злочинця; соціально-психологічний портрет.

Вступ

З розвитком інтернет-технологій, глобалізації, переходом різних сфер діяльності особи в мережу Інтернет (онлайн покупки, участь у соціальних мережах Facebook, LinkedIn, Instagram, Swarm і програмах спілкування Skype, Viber, Whatsapp тощо) чимало особистої інформації з'являється у відкритому доступі. Перегляд в Інтернеті статей, передач, роликів залишає електронний слід. Серед користувачів Інтернету поширеними є «клік або лайк» (від англ. like – «подобається, схвалюю») – це умовне вираження схвалення матеріалу, опублікованого користувачем. Репост здійснюють для збереження потрібного або цікавого контенту, підвищення популярності публікації або поширення рекламної інформації, що створює своєрідний емоційний фон, засвідчує відповідне ставлення людини до чогось (Ozkaya, & Islam, 2019, p. 95). Це своєю чергою надає можливість шахраям дізнатися про вподобання, смаки, проблеми та потреби кожної особи. Поширеними є випадки, коли в соціальних мережах люди зазначають інформацію про місце роботи, день народження, контакти, викладають свої фотографії, а також починають знайомитися. Інтернет-шахраї використовують ці дані для подальшого отримання доступу до грошей жертви.

Постійне вдосконалення мережі Інтернет відбувається в процесі кардинальної трансформації сфер праці, дозвілля та політики. Однак те, що часто називають кіберпростором – цариною комп'ютеризованої взаємодії, – дає змогу вчиняти широкий спектр потенційно злочинних діянь, Інтернет стає провідником злочинності (Brooks). Застосування глобальної мережі надає шахраям лише інший інструмент. Злочини, які вчиняють через використання Інтернету, – це ті самі ненасильницькі традиційні злочини, які набувають нової форми ("The Torpig Trojan", 2009, p. 329).

Кіберзлочинці стають дедалі стійкішими, підвищують рівень професіоналізму ("Cyber-criminals becoming", 2014 p. 1). Інтернет-шахраї «заробляють гроші», намагаються максимально знизити їх простежуваність, однак переказ коштів залишає сліди, і їх можуть використати правоохоронні органи для затримання кіберзлочинців (Ozkaya, & Islam, 2019, p. 95).

Кількість кіберзлочинів в Україні щороку збільшується на тисячі. Найпоширеніший вид злочину – шахрайство в мережі Інтернет. Кіберполіцейські виявили 2798 таких шахрайств, з яких у 2314 випадках було пред'явлено підозри про вчинення злочину. Шахраї створюють сайти та продають товар, якого насправді немає, значна

кількість злочинів стосується виманювання інформації з карток та онлайн кредитування (Hrynchak, 2018, p. 1). Кількість скарг стосовно шахрайств в Інтернеті як на внутрішньому, так і на міжнародному рівнях щороку збільшується. Виманюють кошти з банківських карток, дані з комп'ютерів, інформацію з телефонів, запускають віруси-вимагачі, шантажують компанії та здійснюють криптоафери – це орієнтовний перелік злочинів, які вчиняють інтернет-шахраї.

Встановити особу злочинця у віртуальному світі надто складно. Оскільки злочинець особисто не контактує зі своєю жертвою, а здійснює злочинні дії за допомогою телефонних розмов, SMS та Інтернет-листування. Проблематично також відстежити місцеперебування зловмисника, зокрема, найважливішим елементом під час розслідування звичайного злочину є як місце події, так і сліди, що особа залишає, пересуваючись місцем події. Це ускладнює процес розслідування, оскільки віртуальне злочинне діяння не виявляється в матеріальному світі (Barney, 2018, p. 488).

Особа злочинця є об'єктом дослідження кримінології, криміналістики, юридичної психології та інших наук. Її вивчали такі вчені: І. Антонов, Р. Бєлкін, П. Біленчук, М. Букаєв, І. Возгрін, А. Волобуєв, В. Гаєнко, В. Журавель, В. Коновалова, О. Колесниченко, В. Образцов, В. Тіщенко, М. Селіванов, В. Шепітько та ін. Однак питання вчинення шахрайства з використанням мережі Інтернет досліджено недостатньо. Тому розслідування таких злочинів проводять в умовах інформаційної недостатності. Це засвідчує необхідність удосконалення правоохоронної діяльності з позиції висвітлення відомостей про особу шахрая (Pavlova, Ptushkin, & Chaplynskyi, 2019, p. 41).

Інтернет-шахрайство, на думку фахівців (Ю. Батуріна, Д. Зикова, С. Самойлова, С. Спіріна, С. Чернявського та інших), є різновидом традиційного шахрайства й передбачає заволодіння чужим майном або набуття права на майно шляхом обману та зловживання довірою, його вчиняють з використанням мережі Інтернет, що надає доступ до різноманітних інформаційних ресурсів.

Питання суб'єктів злочинної діяльності у сфері використання мережі Інтернет розглядали у своїх роботах вітчизняні й іноземні науковці: П. Андрушко, В. Вехов, О. Бабенко, П. Біленчук, О. Коваль, В. Козлов, В. Крилов, Г. Левицький, В. Лукашевич, А. Мокляк, Н. Розенфельд, Ю. Степанов, С. С. Чернявський, Д. В. Швець та ін. Попри безумовну теоретичну та практичну важливість цих досліджень, психологічні засади науково обґрунтованого вивчення портрета кіберзлочинця недостатньо висвітлено. Нині майже немає досліджень щодо психологічного портрета особи, яка вчиняє шахрайства в мережі Інтернет. Окреслену тематику комплексно не було розглянуто, суб'єктивно особистісні властивості інтернет-шахрая вивчено недостатньо, що ускладнює процес розслідування цих злочинів.

Подальше дослідження та розроблення соціально-психологічного портрета злочинця, який вчиняє шахрайства в мережі Інтернет, є актуальним і становить не лише теоретичне, а й практичне значення. Можливість визначення соціально-психологічних даних про особу інтернет-шахрая є одним із головних факторів як у розслідуванні злочину, так і в організації заходів протидії та профілактиці таких злочинів. Поінформованість про властивості особистості суб'єктів злочинної діяльності у сфері вчинення інтернет-шахрайств дає змогу оперативним працівникам, слідчим своєчасно виявляти, розслідувати такі злочини, визначати тактику проведення допиту, криміналістичних операцій (Azzneurova, 2010, p. 121).

Мета і завдання дослідження

Мета статті – висвітлити соціально-психологічну характеристику особи, яка вчиняє шахрайства в мережі Інтернет.

Для реалізації мети окреслено такі завдання:

– встановити характерні соціальні та психологічні особливості осіб, які вчиняють шахрайства та злочини в мережі Інтернет;

– сформувати соціально-психологічний портрет особи, яка вчиняє шахрайства в мережі Інтернет;

– висвітлити значення соціально-психологічного портрета особи, яка вчиняє шахрайства в мережі Інтернет в організації заходів протидії таким злочинам.

Виклад основного матеріалу

Головними ознаками інтернет-шахрайства є високий ступінь латентності, багатоманітність способів учинення шахрайства (пов'язано із широким спектром послуг у мережі Інтернет), глобальний характер (інформаційний простір, на відміну від фізичного, не має чітких кордонів й обмежень), складнощі виявлення та запобігання (Cherniavskyi, 2010, p. 100).

Інтернет-шахрайство передбачає дві складові – психологічну й технологічну. Психологічна складова впливає на мотивацію потенційної жертви та спонукає її до вчинення дій, яких очікують шахраї. Відповідними засобами впливу можуть бути: прагнення до одержання матеріальної вигоди (швидке збагачення – основа шахрайських пропозицій); спроба безкоштовно отримати платні послуги чи товари; бажання придбати предмети, які складно чи неможливо придбати в інший спосіб (різноманітні види «аукціонного шахрайства» та продажу товарів, яких немає); альтруїзм (невідомий розповідає

потенційній жертві, що з його близькою людиною сталося лихо).

Технологічна складова надає можливість шахраям, по-перше, передати необхідну інформацію потенційній жертві, по-друге, забезпечити власну анонімність і безпеку, по-третє, одержати від жертви кошти, безпосередньо не контактуючи з нею (Cherniavskyi, 2010, p. 100).

Інтернет – це зручний інструмент у руках шахраїв завдяки величезній аудиторії користувачів і можливості залишатися анонімом (Holubiev, Havlovskyi, & Tsymbaliuk, 2002, p. 7). Анонімність злочинців створює ілюзію безкарності та стимулює дедалі більшу кількість зловмисників, які мають певні навички роботи з комп'ютерними системами, на вчинення цього різновиду злочину. У комп'ютерну злочинність втягнуто широке коло осіб – від кваліфікованих фахівців до дилетантів. Правопорушники приходять з усіх сфер життя і мають різний рівень підготовки (Hovorushka, & Stepanov, 2010, p. 137). Маючи певний досвід, будь-хто з власної квартири або офісу може знайти спосіб обману через Інтернет (Holubiev, Havlovskyi, & Tsymbaliuk, 2002, p. 17).

Анонімність 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 (Shvets, 2016, p. 119). Науковець С. Анненков, характеризуючи особу шахрая, зазначає, що сутність людини як особистості полягає насамперед у тому, що вона є носієм свідомості. Отже, вплив навколишньої дійсності на особистість опосередкований її внутрішнім світом. Особистість є вираженням суспільних відносин. Поняття «особистість» охоплює психологічний склад людини, її спосіб життя й індивідуальні риси (Annenkov,1981, p. 20).

Згідно з дослідженням, проведеним К. М. Євдокімовим, який за ціннісними орієнтаціями, що характеризують спрямованість особистості загалом, визначає ставлення людини до всіх сфер життя, пропонує виокремити такі типи кіберзлочинців:

– *соціально дезадаптивний тип* – особи, характерними рисами яких є аутизація та інтровертність, тобто заглиблення в себе, відмежування від інших, спрямованість інтересів лише на задоволення власних, переважно інформаційних потреб. Для них важливо вважати себе приналежними до класу «хакерів», тобто ототожнювати себе з однією з нечисленних, проте соціальних груп. Вони внутрішньо прагнуть подолати своє соціальне відчуження. Щоб позбутися власного психологічного дискомфорту, особи цього типу легко піддаються сторонньому негативному впливу, переймають злочинний спосіб життя;

– *емоційно сприятливий тип* – особи, які долучилися до вчинення кіберзлочинів для задоволення власних потреб (матеріальних, зрідка – у знаннях). На відміну від правопорушників першого типу, це особи, яким притаманні лідерські якості, з високим рівнем інтелекту. Вони виявляють енергійність й активність, досягаючи своєї мети, гнучкість і легкість у спілкуванні, встановленні соціальних контактів. Однак досягнення мети «будь-яким» шляхом викликає відчуття переваги та презирливе ставлення до інших. Їм необхідний реальний успіх, щоб задовольнити свої потреби. Для них характерні мінливість, відсутність прихильностей до кого-небудь, навіть до рідних, близьких, несприйняття й нерозуміння честі, гідності, обов'язку, нігілізм стосовно правових і моральних норм. Інтернет-шахраї належать до цього типу злочинців;

– *соціально неадекватний тип* формують переважно молоді люди з вищою освітою, високим інтелектуальним рівнем, а також матеріально забезпечені. Корисливі мотиви й матеріальні потреби не відіграють важливої ролі, насамперед слід задовольнити нематеріальні. Надмірні або незрозумілі з позиції інших, проте природні, як вважає злочинець, запити формують потребу «промотиваційної» сфери, яку неможливо дозволити через особисте небажання та прийняття встановлених правових (соціальних) норм. Психологічного комфорту й позбавлення напруженості досягають за допомогою цілеспрямованої діяльності, що призводить до бажаних результатів (Evdokimov, 2006, p. 120).

Більшість інтернет-шахраїв належать до другого типу соціальної спрямованості, проте визначальним фактором їх ціннісно-орієнтаційної сфери є корислива спрямованість особистості (Kravtsova, 2015, p. 51).

На нашу думку, інтернет-шахраї мають стійку підсвідому антисоціальну спрямованість, зазіхаючи на основне надбання суспільства – розподіл матеріальних благ відповідно до виконаної праці. Такі злочини вчиняють з прямим умислом. Мотивація кібершахраїв – бажання отримати «легкі гроші», довести власну значущість, настанова на задоволення власних корисливих потреб шляхом маніпуляції з жертвою, чітка усвідомлена настанова на збагачення та життєвий успіх (Irkhin, 2010, p. 388). До зазначеного переліку можна віднести не лише користь, а й помсту та самоствердження.

Кібершахраї здебільшого не вчиняють інтернет-шахрайства одноразово. Шахрайство – це складова елементів трикутника: мотив, можливості, раціональність. Підґрунтям шахрайства є емоційний вплив на жертв. «Професійні» звички та почерк злочинців виражені певними способами, методами, прийомами вчинення злочинів.

Залишені на місці злочину сліди засвідчують особливості його соціально-психологічного портрета: досвід, професія, вік, стать, знання тощо. Формування банку типових моделей різних категорій злочинців дасть змогу оптимізувати процес виявлення кола осіб, серед яких найбільш вірогідний пошук злочинця (Nykyforchuk, 2013, p. 181). Зібрані в процесі розслідування відомості про особу злочинця, його кримінальну поведінку та злочинні дії створюють фактичну базу прийняття обґрунтованих правових рішень для його переслідування (Padgett, 2014, p. 55).

Дослідник Л. Прудка зазначає, 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 стисліший строк тощо) (Prudka, 2018, p. 31).

Особистісними характеристиками портрета комп'ютерного злочинця є активна життєва позиція, нестандартність мислення та поведінки, обережність, уважність, креативність, реакція вибору (з попередньою оцінкою ситуації) і реакція на небезпеку, здатність витримувати інтенсивне тривале психоемоційне навантаження без зниження продуктивності злочинної діяльності, розвинута уява, інтелектуальна ініціативність. Це зазвичай яскрава, розумна і творча особистість. Її поведінка зрідка відрізняється від визначених у суспільстві соціальних стандартів і норм поведінки.

Практика засвідчує, що більшість комп'ютерних злочинців не мають кримінального минулого, майже ніхто з обвинувачених інтернет-шахраїв на обліках не перебував. Визначальною характеристикою інтернет-шахрая є те, що для вчинення цих злочинів не потрібна спеціальна освіта у сфері комп'ютерних технологій, вважає П. Біленчук, 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 (Bilenchuk, 2001, p. 15).

Осіб, які вчиняють кібершахрайства, переважно позитивно характеризують за місцем роботи й мешкання.

Згідно зі статистичними даними, більшість кіберзлочинів проти власності (79 %) – це шахрайства, учинені чоловіками (94 %). Такі злочини вчиняють здебільшого особи, які офіційно не перебувають у шлюбі та не мають дітей. Кількість неодружених осіб становить 70 %, одружених – 30 %. Згідно з даними судової практики, 51 % осіб, які вчинили кіберзлочини, не мають постійного місця роботи, такі особи вчиняють зазвичай шахрайства. Серед решти 49 % більшість становлять менеджери нижчої та середньої ланок, рідше – посадові особи та програмісти. Якщо середній вік шахрая в матеріальному світі становить 26–39 років, то середній вік кібершахрая – від 18 до 40 років. Соціальне становище в суспільстві – від студента до співробітника державної установи або фірми (Pitsyk, 2017, p. 106). Учинення шахрайства під час спілкування телефоном потребує спеціальних умінь, щоб викликати довіру людей. Наприклад, у м. Запоріжжі працівники шахрайського офісу (штат співробітників – близько 100 осіб, серед яких були неповнолітні) виманювали у громадян CVV-код, номер картки, пін-код тощо. Для цього вони використовували також психологічні методи впливу та діяли за інструкцією. Крім того, щомісяця всі співробітники call-центру проходили відповідні тренінги, отримували інструкції для спілкування з клієнтами, перекладені чотирма мовами. Щодня кожен співробітник здійснював близько сотні таких дзвінків. Отриману інформацію використовували для викрадення грошей із банківських карток потерпілих ("Kiberpolitsiia prypynyla diialnist", 2019). Кіберзлочинці – це актори зі складною організацією діяльності (Howard, 2009, p. 500).

Характеристику особи злочинця становлять ті дані, за якими можна визначати ефективні шляхи розшуку та викриття злочинця. Під час дослідження особи злочинця важливу роль відіграють як сліди, залишені ним у процесі вчинення злочину, так й інформація про соціально-психологічні риси особи, що дає змогу звузити коло пошуку, виокремити категорії, групи людей і навіть конкретних осіб, які мають унікальні особливості, що є досить складним упродовж розслідування віртуального злочину.

Зокрема, І. Котюк і П. Біленчук характерними соціально-психологічними ознаками особи типового шахрая вважають: 1) поінформованість про різні сфери людської діяльності; 2) визначальний мотив злочину – користь. Зіставляючи таку характеристику з віком типового інтернет-шахрая (близько 18–40 років, водночас основний відсоток припадає на віковий період

з 18 до 25 років), можна дійти висновку, що типовий інтернет-шахрай – студент ЗВО або установи середньої професійної освіти, який не працює і, можливо, перебуває на утриманні батьків або інших родичів; 3) розвинені комунікативні риси, винахідливість, спостережливість. Також було зафіксовано випадки, коли чоловіки-злочинці успішно спілкувалися в Інтернеті зі своїми жертвами від імені жінок (такі випадки трапляються переважно в шлюбних аферах з використанням сайтів знайомств); 4) чимало шахраїв не перебувають у шлюбі (Kotiuk, & Bilenchuk, 2007, p. 65).

Зв'язок особи злочинця та способу вчинення злочину слід характеризувати однозначно: ознаки першої визначають характер другого, оскільки спосіб не може виходити за межі, окреслені психологічними та фізичними властивостями особи або групи осіб (Cherniavskyi, 2010, p. 226).

Наявні також певні особливості особистості, що обумовлюють вибір конкретної злочинної діяльності, яку шахрай планує вчиняти. Тому за видом інтернет-шахрайства, учиненого злочинцем, можна визначити психологічні властивості особи та запропонувати її психологічний портрет. Таким чином, під час розслідування конкретних злочинів коло можливих суб'єктів можна істотно звузити.

Підсумовуючи зазначене, можна сформувати *типовий портрет особи, яка вчиняє шахрайства в мережі Інтернет*: чоловік, який ніде не працює або не має постійного місця роботи, віком 20–35 років, офіційно неодружений, не має дітей, успішний, не був притягнутий до кримінальної відповідальності, неконфліктний, не зловживає алкоголем, його позитивно характеризують за місцем мешкання, впевнений у собі, інтелектуально розвинутий, ввічливий, справляє позитивне враження в спілкуванні, артистичний, творчий.

Під час складання *психологічного портрета* відмітними рисами для інтернет-шахрая слід вважати: схильність до авантюризму (постійний ризик є фізіологічно необхідним для шахрая), рішучість, знижена тривожність, терпимість, обережність, самоконтроль у різних ситуаціях, уважність, планомірність, внутрішня організованість, емпатійність (уміння поставити себе на місце іншої людини, здатність відчувати внутрішній світ жертви й розуміти її психічні стани), інтуїтивність, розвинена уява, вміння викликати довіру, знаходити слабкі сторони жертви, прогнозувати поведінку та застосовувати способи маніпуляції.

Важливою властивістю особи злочинця є усвідомлена настанова – прагнення збагатитися, жадібність ("Profiling Individual", 2015, p. 95). З-поміж с*успільно спрямованих якостей* інтернет-шахрая слід виокремити егоцентризм, зневагу до інтересів і думок деяких членів суспільства, відсутність жалю до жертви (через відчуття віртуальності), легкість встановлення соціальних контактів, гнучкість у спілкуванні. В умовах анонімності інтернет-шахрай відчуває можливість безкарно здійснювати негативні вчинки, водночас відсутність ефективних механізмів осуду посилює це бажання. Відчуття безкарності не лише впливає на окремих осіб, а й створює атмосферу вседозволеності, яка сприяє подальшому поширенню й розвитку суспільно небезпечних ідей (Shvets, 2018, p. 119).

Наукова новизна

На підставі аналізу позицій вітчизняних й іноземних учених щодо характеристики портрета кіберзлочинця та шахрая запропоновано типовий портрет особи, яка вчиняє шахрайства в мережі Інтернет. Сформовано типовий соціально-психологічний портрет злочинця відповідно до виду вчиненого інтернет-шахрайства, окреслено його роль у розслідуванні таких злочинів. Соціально-психологічна характеристика інтернет-шахрая надасть можливість визначити основні соціально-психологічні риси, притаманні суб'єктам злочинної діяльності у сфері вчинення інтернет-шахрайств, оптимізувати процес виявлення кола осіб, серед яких доцільно вести пошук злочинця, і викрити конкретного правопорушника. Крім цього, вона є важливим інструментом в організації заходів протидії та профілактики таких злочинів.

Висновки

Згідно з даними звітів правоохоронних органів, галузевих опитувань і наукових досліджень, рівень кібершахрайства протягом останнього десятиліття зростає експоненціально щороку з позиції кількості випадків і розміру завданої шкоди. Кібершахрайства стали такими поширеними, що їх вплив на будь-яку сферу особистих або організаційних стосунків неможливо мінімізувати. Наслідки таких злочинів ставлять під загрозу довіру, фінанси, конфіденційність і добробут населення, установ та організацій (Balogun, & Zuva, 2017, p. 143).

З метою збагачення інтернет-шахраї використовують злочинні прийоми, що призводить до негативних наслідків, оскільки їхніми жертвами стають не лише пересічні громадяни, а й приватні та державні організації, банківські установи (шкодять нормальному функціонуванню банківської системи, здійсненню банками кредитних операцій, а також є серйозною загрозою для страхового ринку тощо) (Dorokhina, & Iliashko, 2019, p. 91).

Для більшості організацій очевидним результатом шахрайства є фінансові втрати. Усвідомлення можливості їх настання може

допомогти в профілактиці ризику шахрайства ("Profiling Individual", 2015, p. 148).

Щоб спіймати шахрая, слід мислити як він, знати його психологічні особливості поведінки. Це надає можливість зрозуміти методологію формування шахрайства, ураховуючи основні його елементи – мотив, можливість, раціональність. Профілювання інтернет-шахраїв є практичним інструментом для постійного використання слідчими під час розслідування таких злочинів і потребує об'єднання інформації з різних джерел, зокрема особистих відомостей про злочинця, даних про спосіб злочинних дій, мотив злочинця та можливості вчинити злочин ("Profiling Individual", 2015, p. 197).

Необхідно визначити соціально-психологічні риси, притаманні інтернет-шахраям. Встановити злочинця у віртуальному світі складно. Кіберзлочинці повсякчас підвищують рівень професіоналізму, удосконалюючи способи вчинення та приховування злочинів. Є певні особливості особистості, що зумовлюють вибір конкретної злочинної діяльності. Маючи соціально-психологічну характеристику особи інтернет-шахрая, можна скласти соціально-психологічний портрет відповідно до вчиненого інтернет-шахрайства й окреслити ефективні шляхи його викриття, оптимізувати процес виявлення кола осіб, серед яких слід вести пошук злочинця, і визначити правопорушника. Встановлені особливості портрета інтернет-шахрая є підґрунтям для розслідування злочину, організації заходів протидії та профілактики шахрайств, що вчиняють за допомогою мережі Інтернет (Azzneurova, 2010, p. 121; Padgett, 2014).

Соціально-психологічна характеристика поведінки особи, яка вчиняє шахрайства в мережі Інтернет, сприятиме вдосконаленню методів розслідування таких шахрайств і вчасному їх виявленню.

REFERENCES

Annenkov, S.I. (1981). Kriminalisticheskie sredstva i metody borby s khishcheniiami gosudarstvennogo ili obshchestvennogo imushchestva, sovershaemye putem moshennichestva [Forensic tools and methods of combating theft of state or public property committed through fraud]. *Extended abstract of candidate's thesis.* Saratov [in Russian].

Azzneurova, G.G. (2010). Nekotorye osobennosti lichnosti "kompiuternogo prestupnika" [Some features of the personality of a "computer criminal"]. *Protydiia zlochynnosti u sferi intelektualnoi vlasnosti ta kompiuternykh tekhnolohii orhanamy vnutrishnikh sprav: stan, problemy ta shliakhy vyrishennia, Anti-crime in the Sphere of Intellectual Property and Computer Technologies by the Law Enforcement Agencies: State, Problems and Solutions:* Proceedings of the All-Ukrainian Scientific and Practical Conference (pp. 121-123). Donetsk: Donetsk. yuryd. in-t LDUVS im. E.O. Didorenko [in Ukrainian].

Balogun, A.M., & Zuva, T. (2017). Open issues in cybercriminal profiling. *2017 1st International Conference on Next Generation Computing Applications (NextComp),* 141-145. doi: 10.1109/nextcomp.2017.8016189.

Barney, Warf. (2018). Internet Fraud. *The SAGE Encyclopedia of the Internet,* 488-493. doi: 10.4135/9781473960367.n144.

Bilenchuk, P.D. *Pytannia sotsialnoi ta kryminalistychnoi kharakterystyky kompiuternoho zlochyntsia [Questions of social and forensic characteristics of a computer offender].* Retrieved from http://www.crime-research.ru/library/Bilen3.htm [in Ukrainian].

Brooks, G. Internet Fraud. *The SAGE Encyclopedia of the Internet.* B. Warf (Eds.). doi: 10.4135/9781473960367.n144.

Cherniavskyi, S.S. (2010). *Finansove shakhraistvo: metodolohichni zasady rozsliduvannia [Financial Fraud: Methodological Basis of Investigation].* Kyiv [in Ukrainian].

Cherniavskyi, S.S. (2010). Internet shakhraistvo yak obiekt doslidzhennia pravovykh nauk [Internet fraud as a subject of research of legal sciences]. *Protydiia zlochynnosti u sferi intelektualnoi vlasnosti ta kompiuternykh tekhnolohii orhanamy vnutrishnikh sprav: stan, problemy ta shliakhy vyrishennia, Counteraction to crime in the field of intellectual property and computer technologies by law enforcement agencies: state, problems and solutions:* Proceedings of the all-Ukrainian Scientific and Practical Conference (pp. 100-103). Donetsk: DIuI: LDUVS [in Ukrainian].

Computer and Internet Fraud: A Risk Identification Overview. (2003). *Computer Fraud & Security, 6,* 6-9. doi: 10.1016/s1361-3723(03)06008-1.

Cyber-criminals becoming more professional. (2014). *Computer Fraud & Security, 1,* 3. doi: 10.1016/s1361-3723(14)70003-x.

Dorokhina, Yu.A., & Iliashko, A.O. (2019). Okremi problemy rozmezhuvannia shakhraistva ta shakhraistva z finansovymy resursamy [Separate Problems of Separating Fraud and Fraud with Financial Resources]. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho, Notes of the Taurida V.I. Vernadsky National University, 30(69), 3,* 91-94. doi: https://doi.org/10.32838/1606-3716/2019.3/16 [in Ukrainian].

Evdokimov, K.N. (2006). Ugolovno-pravovye i kriminalisticheskie aspekty protivodeystviia nepravomernomu dostupu k kompiuternoy informatsii: po materialam Vostochno-Sibirskogo regiona [Criminal-legal and forensic aspects of counteracting illegal access to computer information: according to the materials of the East Siberian region]. *Candidate's thesis.* Irkutsk [in Russian].

Fraud Profiling Your Organization. (2015). *Profiling the Fraudster,* 197-204. doi: 10.1002/9781118929773.ch20.

Holubiev, V.O., Havlovskyi, V.D., & Tsymbaliuk, V.S. (2002). *Problemy borotby zi zlochynnistiu u sferi vykorystannia kompiuternykh tekhnolohii [Problems of combating crime in the field of computer technology usage].* R.A. Kaliuzhnyi (Eds.). Zaporizhzhia: ZIDMU [in Ukrainian].

Hovorushka, V.O., & Stepanov, Yu.V. (2010). Sotsialna ta kryminalistychna kharakterystyka kompiuternoho zlochyntsia [Social and forensic characteristics of a computer offender]. *Protydiia zlochynnosti u sferi intelektualnoi vlasnosti ta kompiuternykh tekhnolohii orhanamy vnutrishnikh sprav: stan, problemy ta shliakhy vyrishennia, Counteraction to crime in the field of intellectual property and computer technologies by law enforcement agencies: state, problems and solutions:* Proceedings of the all-Ukrainian Scientific and Practical Conference (pp. 137-140). Donetsk: DIuI: LDUVS [in Ukrainian].

How to Act Like a Fraudster: To Catch a Fraudster, You Need to Think Like One. (2013). *Detecting Fraud in Organizations,* 155-183. doi: 10.1002/9781118555972.ch4.

Howard, R. (2009). *Cyber Fraud: Tactics, Techniques and Procedures.* doi: 10.1201/9781420091281.

Hrynchak, A. (2018). *Shcho varto znaty pro kiberzlochyntsiv v Ukraini [What to Know About Cybercriminals in Ukraine].* Retrieved from https://www.radiosvoboda.org/a/details/29031166.html [in Ukrainian].

Irkhin, Yu.B. (2010). Psykholohichni zasady dovirlyvosti u shakhraistvi yak element delikventnoho povodzhennia osobystosti [Psychological principles of trust in fraud as an element of delinquent behavior of the individual]. *Problemy suchasnoi psykholohii, Problems of modern psychology, 8,* 388-397 [in Ukrainian].

Kiberpolitsiia prypynyla diialnist shakhraiskoho call-tsentru zi shchotyzhnevym obihom u 3 miliony hryven [Cyber police stop fraudulent call center with weekly turnover of UAH 3 million]. (n.d.). *cyberpolice.gov.ua.* Retrieved from https://cyberpolice.gov.ua/news/kiberpolicziya-prypynyla-diyalnist-shaxrajskogo-call-czentru-zi-shhotyzhnevym-obigom-u--miljony-gryven-6263 [in Ukrainian].

Kotiuk, I.I., & Bilenchuk, P.D. (2007). Kompiuterna zlochynnist v bankivskii industrii [Computer crime in the banking industry]. *Borotba zi zlochynamy u sferi kompiuternoi informatsii: problemy ta shliakhy yikh vyrishennia, Combating crime in the field of computer information: problems and ways of solving them: materials of the university*: Proceedings of the Intercollegiate Scientific and Practical Conference (pp. 65-69). Donetsk: Donetsk. yuryd. in-t [in Ukrainian].

Kravtsova, M.O. (2015). Suchasnyi kiberzlochynets: kryminolohichna kharakterystyka osobystosti [Modern Cybercriminals: Criminological Characteristics of Personality]. *Mytna sprava, Customs Case, 4(100), 2,* 46-53 [in Ukrainian].

Nykyforchuk, V.D. (2013). Kharakterystyka osoby kiberzlochyntsia [Characteristics of a cybercriminal person]. *Pravovi reformy v Ukraini, Legal reforms in Ukraine, 1,* 181-181. Retrieved from http://elar.naiau.kiev.ua/bitstream/f [in Ukrainian].

Ozkaya, E., & Islam, R. (2019). Cybercriminal Activities in Dark Net. *Inside the Dark Web,* 95-120. doi: 10.1201/9780367260453-6.

Padgett, S. (2014). *Profiling the Fraudster: Removing the Mask to Prevent and Detect Fraud.* 2014. doi: 10.1002/9781118929773.

Pavlova, N.V., Ptushkin, D.A., & Chaplynskyi, K.A. (2019). *Teoretychni zasady metodyky rozsliduvannia shakhraistva, poviazanoho z vidchuzhenniam obiektiv nerukhomoho maina hromadian [Theoretical foundations of the method of investigation of fraud related to alienation of objects of real estate of citizens].* Dnipro: Dnipropetr. derzh. un-t vnutr. sprav [in Ukrainian].

Pitsyk, Yu.M. (2017). Analiz osobystosti kiberzlochyntsia yakyi vchyniaie zlochyny proty vlasnosti u kiberprostori [Analysis of the identity of a cyber criminal who commits crimes against property in cyberspace]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu, Scientific Bulletin of the International Humanities University, 26,* 105-107 [in Ukrainain].

Profiling Individual Behavior and Characteristics of a Fraudster. (2015). *Simon Padgett Profiling the Fraudster,* 95-111. doi: 10.1002/9781118929773.ch11.

Profiling the Consequences. (2015). *Profiling the Fraudster,* 147-152. doi: 10.1002/9781118929773.ch15.

Prudka, L.M. (2018). Psykholohichni osoblyvosti shakhraistva v merezhi Internet [Psychological features of fraud in the Internet]. *Pivdennoukrainskyi pravnychyi pravopys, South Ukrainian legal spelling, 2,* 30-33. Retrieved from http://www.sulj.oduvs.od.ua/archive/2018/2/10.pdf [in Ukrainian].

Shvets, D.V. (2018). Pidkhody do vyznachennia psykholohichnoho portreta kiberzlochyntsia [Approaches to definition of a psychological portrait of a cybercriminal]. *Aktualni pytannia protydii zlochynnosti ta torhivlia liudmy, Topical issues of combating crime and human trafficking:* Proceedings of the All-Ukrainian Scientific and Practical Conference (pp. 118-121). Kharkiv: Kharkiv. nats. un-t vnutr. sprav [in Ukrainian].

The Accidental Fraudster (Bad Apple): When the Apple Turns and Honesty Reverses Course. (2013). *A.B.C.'s of Behavioral Forensics,* 121-141. doi: 10.1002/9781118740422.ch6.

The Fraudster Mindset. (2013). *Faces of Fraud,* 1-21. doi: 10.1002/9781118556917.ch1.

The Torpig Trojan Exposed. (2009). *Cyber Fraud,* 329-348. doi: 10.1201/9781420091281.ch10.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Анненков С. И. Криминалистические средства и методы борьбы с хищениями государственного или общественного имущества, совершаемые путем мошенничества : автореф. дис. … канд. юрид. наук : 12.00.09. Саратов, 1981. 20 с.

Азжеурова Г. Г. Некоторые особенности личности «компьютерного преступника». *Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми*

та шляхи вирішення : тези доп. Всеукр. наук.-практ. конф. (Донецьк, 12 листоп. 2010 р.). Донецьк : Донецьк. юрид. ін.-т ЛДУВС ім. Е. О. Дидоренка, 2010. С. 121–123.

Balogun A. M., Zuva T. Open issues in cybercriminal profiling. *2017 1st International Conference on Next Generation Computing Applications (NextComp).* 2017. P. 141–145. doi: 10.1109/nextcomp.2017.8016189.

Barney Warf Internet Fraud. *The SAGE Encyclopedia of the Internet.* 2018. P. 488–493. doi: 10.4135/9781473960367.n144.

Біленчук П. Д. Питання соціальної та криміналістичної характеристики комп'ютерного злочинця. URL: http://www.crime-research.ru/library/Bilen3.htm.

Brooks G. Internet Fraud. *The SAGE Encyclopedia of the Internet* / Edited by B. Warf. doi: 10.4135/9781473960367.n144.

Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ, 2010. 624 с.

Чернявський С. С. Інтернет шахрайство як об'єкт дослідження правових наук. *Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення* : матеріали Всеукр. наук.-практ. конф. (Донецьк, 12 листоп. 2010 р.). Донецьк : ДЮІ ЛДУВС, 2010. С. 100–103.

Computer and Internet Fraud: A Risk Identification Overview. *Computer Fraud & Security.* 2003. No. 6. P. 6–9. doi: 10.1016/s1361-3723(03)06008-1.

Cyber-criminals becoming more professional. *Computer Fraud & Security.* 2014. No. 1. P. 3. doi: 10.1016/s1361-3723(14)70003-x.

Дорохіна Ю. А., Іляшко А. О. Окремі проблеми розмежування шахрайства та шахрайства з фінансовими ресурсами. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* 2019. Т. 30 (69). № 3. С. 91–94. doi: https://doi.org/10.32838/1606-3716/2019.3/16.

Евдокимов К. Н. Уголовно-правовые и криминалистические аспекты противодействия неправомерному доступу к компьютерной информации: по материалам Восточно-Сибирского региона : дис. … канд. юрид. наук : 12.00.08. Иркутск, 2006. 203 с.

Fraud Profiling Your Organization. *Profiling the Fraudster.* 2015. P. 197–204. doi: 10.1002/9781118929773.ch20.

Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинністю у сфері використання комп'ютерних технологій : навч. посіб. / за заг. ред. Р. А. Калюжного. Запоріжжя : ЗІДМУ, 2002. 292. с.

Говорушка В. О., Степанов Ю. В. Соціальна та криміналістична характеристика комп'ютерного злочинця. *Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення* : матеріали Всеукр. наук.-практ. конф. (Донецьк, 12 листоп. 2010 р.) Донецьк : ДЮІ ЛДУВС, 2010. С. 137–140.

How to Act Like a Fraudster: To Catch a Fraudster, You Need to Think Like One. *Detecting Fraud in Organizations.* 2013. P. 155–183. doi: 10.1002/9781118555972.ch4.

Howard R. Cyber Fraud: Tactics, Techniques and Procedures. 2009. 504 p. doi: 10.1201/9781420091281.

Гринчак О. Що варто знати про кіберзлочинців в Україні. 2018 URL: https://www.radiosvoboda.org/a/details/29031166.html.

Ірхін Ю. Б. Психологічні засади довірливості у шахрайстві як елемент делінквентного поводження особистості. *Проблеми сучасної психології.* 2010. Вип. 8. С. 388–397.

Кіберполіція припинила діяльність шахрайського call-центру зі щотижневим обігом у 3 мільйони гривень. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-prypynyla-diyalnist-shaxrajskogo-call-czentru-zi-shhotyzhnevym-obigom-u--miljony-gryven-6263.

Котюк І. І., Біленчук П. Д. Комп'ютерна злочинність в банківській індустрії. *Боротьба зі злочинами у сфері комп'ютерної інформації: проблеми та шляхи їх вирішення* : матеріали міжвузів. наук.-практ. конф. (Донецьк, 14 груд. 2007 р.). Донецьк : Донецьк. юрид. ін-т, 2007. С. 65–69.

Кравцова М. О. Сучасний кіберзлочинець: кримінологічна характеристика особистості. *Митна справа.* 2015. № 4 (100). Ч. 2. С. 46–53.

Никифорчук В. Д. Характеристика особи кіберзлочинця. *Правові реформи в Україні.* 2013. Ч. 1. С. 181–181. URL: http://elar.naiau.kiev.ua/bitstream/f.

Ozkaya E., Islam R. Cybercriminal Activities in Dark Net. Inside the Dark Web, 2019. P. 95–120. doi: 10.1201/9780367260453-6.

Padgett S. Profiling the Fraudster: Removing the Mask to Prevent and Detect Fraud. 2014. doi: 10.1002/9781118929773.

Павлова Н. В., Птушкін Д. А., Чаплинський К. О. Теоретичні засади методики розслідування шахрайства, пов'язаного з відчуженням об'єктів нерухомого майна громадян : монографія. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2019. 190 с.

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

Profiling Individual Behavior and Characteristics of a Fraudster. *Simon Padgett Profiling the Fraudster.* 2015. P. 95–111. doi: 10.1002/9781118929773.ch11.

Profiling the Consequences. *Profiling the Fraudster.* 2015. P. 147–152. doi: 10.1002/9781118929773.ch15.

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.

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.
The Accidental Fraudster (Bad Apple): When the Apple Turns and Honesty Reverses Course. *A.B.C.'s of Behavioral Forensics.* 2013. P. 121–141. doi: 10.1002/9781118740422.ch6.
The Fraudster Mindset. *Faces of Fraud.* 2013. P. 1–21. doi: 10.1002/9781118556917.ch1.
The Torpig Trojan Exposed. *Cyber Fraud.* 2009. P. 329–348. doi: 10.1201/9781420091281.ch10.

Стаття надійшла до редколегії 11.12.2019

Bryskovska O. – Ph.D in Law, Senior Research Fellow, Leading Research Fellow of the Scientific Laboratory on the Problems of Combating Crime of the Educational and Research Institute No. 1 of the National Academy of Internal Affairs, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-6902-9969

Socio-Psychological Characteristics of the Person Committing Fraud on the Internet

The urgency of the scientific article. Identifying the criminal in the virtual world is an extremely problematic process. The number of cybercrimes in Ukraine is increasing by several thousand every year. The most common crime is committing frauds in the Internet. Cyber swindlers enhance their professionalism by refining ways to commit and conceal crimes. Most often, scammers create websites and sell non-existent goods. A significant number of crimes are related to the extraction of the information from the bank cards, mobile phones, and computers. Internet scammers launch ransom ware's computer viruses, blackmail companies, and organize frauds with crypto currency. And this is not a complete list of the crimes they commit. The success of preventing such crimes, exposing them and bringing those, who is responsible, to justice is a rare occurrence, if you compare it to the number of such offenses. Socio-psychological characteristics of the behavior of the person who commits fraud on the Internet, will allow to improve the methods of the investigation and to detect such manifestations in advance. The ***purpose*** *of this article is generalization of the socio-psychological characteristics of the person committing fraud on the Internet. This characteristic makes it possible to establish a socio-psychological portrait of the offender in accordance with the type of committed online fraud, which will in crease the effectiveness of investigating such crimes.* ***Methodology*** *sof this science article are coherent and consistent system of methods that made it possible to properly analyze the subject of the study. In particular, there were used scientific methods of analysis, induction and deduction. Summarizing the above, it should be* ***conclusions*** *that there is a certain set of personality traits that determine the choice of a particular criminal activity that the fraudster is about to commit. Established and generalized socio-psychological characteristics of the Internet fraudster will allow to make a socio-psychological portrait in accordance with the committed Internet fraud, to determine the effective ways of exposing it, to optimize the process of identifying the circle of persons among whom it would be worth to search the offender, and to identify the appropriate offender. The revealed socio-psychological features of the Internet fraudster's portrait form the basis for the investigation of the crime and the organization of counteraction and prevention of frauds committed through the Internet.*

Keywords: Internet; Internet fraud; cyber swindler; Internet fraudster; the criminal; socio-psychological portrait.