Кримінальне право та кримінологія; кримінально-виконавче право

УДК 343.85
DOI 10.33244/2617-4154.1(8).2022.151-159

О. М. Бодунова,
канд. юрид. наук, доцент,
Державний податковий університет
e-mail: olesalasuk@gmail.com
ORCID ID 0000-0001-9179-5985

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ОСОБИ, ЩО ВЧИНЯЄ КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

У статті охарактеризовано особу, що вчиняє кримінальні правопорушення у сфері інформаційних технологій. Актуальність обраної теми дослідження зумовлена тим, що стрімкий розвиток технологічного прогресу в останні роки зумовив пришвидшення різних процесів як державного, так і недержавного характеру. Поряд з цим інформаційні технології стали активно використовуватися злочинцями у кримінально протиправних цілях. Це пришвидшує вчинення кримінальних правопорушень, а також дає можливість злочинцям довгий час лишатися «непоміченими» серед правоохоронних органів.

Крім того, кримінальні правопорушення, які вчиняються у сфері інформаційних технологій, характеризуються підвищеною суспільною небезпечністю, адже мають відношення і до інших сфер, зокрема проти власності, національної безпеки, громадської безпеки тощо. Питома вага вищевказаних кримінальних правопорушень, що вчиняються у цих сферах, є у 2–3 рази більшою, ніж 10 років потому. У зв'язку з цим одним з нагальних питань сьогодення є розробка оновленої моделі запобігання злочинності у сфері інформаційних технологій, оскільки остання досить швидко й активно трансформується, злочинці використовують нові методи вчинення кримінальних правопорушень, невідомі правоохоронним органам.

Такий кримінологічний аналіз кримінальних правопорушень, скоєних з використанням інформаційних технологій, та розробка ефективних шляхів і напрямів їх запобігання неможливі без урахування типових особистісних характеристик осіб, які безпосередньо вчиняють кіберзлочини. Саме тому доцільним і актуальним питанням є вивчення ознак особи, що вчиняє кримінальні правопорушення у сфері інформаційних технологій.

У процесі написання наукової статті використовувалися такі методи: діалектичний – для пізнання окремих процесів, явищ; статистичний – під час аналізу офіційних даних щодо осіб, які вчинили кримінальне правопорушення у сфері інформаційних технологій; системний – у разі розгляду видів кіберзлочинців тощо.

Розглянувши наукові праці та дані офіційної статистики, сформульовано типовий кримінологічний портрет особи, що вчиняє кримінальні правопорушення у сфері інформаційних технологій.

Ключові слова: *кіберзлочинці, злочинність у сфері інформаційних технологій, кримінальне правопорушення, соціально-демографічні ознаки, морально-психологічні ознаки, запобігання.*

Метою статті є дослідження типових ознак та властивостей осіб, що вчиняють кримінальні правопорушення у сфері інформаційних технологій для формування ефективної моделі запобігання злочинності у цій сфері.

Постановка проблеми. Стрімкий розвиток технологічного прогресу в останні роки зумовив пришвидшення різних процесів як державного, так і недержавного характеру. Поряд з цим інформаційні технології стали активно використовуватися злочинцями у кримінально протиправних цілях. Це пришвидшує вчинення кримінальних правопорушень, а також дає можливість злочинцям довгий час лишатися «непоміченими» в очах правоохоронних органів.

Крім того, кримінальні правопорушення, які вчиняються у сфері інформаційних технологій, характеризуються підвищеною суспільною небезпечністю, адже мають відношення і до інших сфер, зокрема проти власності, національної безпеки, громадської безпеки тощо. Питома вага вищевказаних кримінальних правопорушень, що вчиняються у цих сферах, є у 2–3 рази більшою, ніж 10 пороків тому. У зв'язку з цим одним з нагальних питань сьогодення є розробка оновленої моделі запобігання злочинності у сфері інформаційних технологій, оскільки остання досить швидко й активно трансформується, злочинці використовують нові методи вчинення кримінальних правопорушень, невідомі правоохоронним органам.

Такий кримінологічний аналіз кримінальних правопорушень, скоєних з використанням інформаційних технологій, та розробка ефективних шляхів і напрямів їх запобігання неможливі без урахування типових особистісних характеристик осіб, які безпосередньо вчиняють кіберзлочини. Саме тому доцільним і актуальним питанням є вивчення ознак особи, що вчиняє кримінальні правопорушення у сфері інформаційних технологій.

Аналіз останніх досліджень і публікацій. Дослідженнями питання запобігання злочинності у сфері інформаційних технологій, розробкою кримінологічної моделі запобігання кіберзлочинів займались такі науковці, як Н. Ахтирська, В. Бутузов, С. Буяджи, В. Гавловський, І. Європіна, О. Іванченко, М. Кравцова, Л. Скалозуб, Є. Скулиш та інші. Проте на сьогодні у кримінології відсутні ґрунтовні праці щодо типового кримінологічного портрета кіберзлочинців. Саме тому у статті нами здійснена спроба висвітлення цього поняття та його ознак.

Виклад основного матеріалу. Питання кримінологічної характеристики особи, що вчиняє кримінальні правопорушення у сфері інформаційних технологій, не є новим. Зокрема, М. О. Кравцова надає кримінологічну характеристику особистості кіберзлочинця. На її думку, кіберзлочинці – це переважно працездатні, але непрацюючі, неодружені чоловіки, й структурі морально-психологічних якостей яких превалюють корисливість, правовий нігілізм, поєднані з детермінованим специфікою кіберпростору комплексом сваволі та ілюзій [1, с. 20]. Хоча дослідження цієї тематики не зупиняються й на сьогодні, адже злочинність у сфері інформаційних технологій постійно розвивається і виходить на новий рівень.

Досліджуючи осіб, які вчиняють кримінальні правопорушення у сфері інформаційних технологій, їх можна розглядати як з точки зору характеристики кримінально протиправних дій, так і з боку характеристики особистості – суб'єктів вчинення кримінальних правопорушень. Так, фахівцями університету Норідж (приватний військовий університет, розташований у Нортфілді, штат Вермонт, США) виділяються такі види кіберзлочинців:

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

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

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

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

Зі свого боку Р. Мітчелл визначив типи кіберзлочинців, які відрізняються своїм рівнем майстерності та мотивацією, зокрема це такі: початківці, кіберпанки, внутрішні (внутрішня загроза), кодери, інформаційні воїни / кібертерористи, старі хакери охорони, професійні кіберзлочинці [3].

Мотиви вчинення кримінальних правопорушень кіберзлочинцями є досить різними. Це насамперед бажання матеріальної наживи, шпигунство, особисті мотиви, саботаж політичних, релігійних чи інших переконань, підвищення самооцінки тощо. У багатьох кіберзлочинців присутній нарцисизм і надмірна «любов» до себе.

Є загальне хибне уявлення щодо кіберзлочинців. Передбачається, що вони мають різноманітні навички та злочинний досвід, який дає змогу їм ініціювати широкий спектр нападів, згодом заробляючи велику кількість грошей. Насправді

нещодавні дослідження, проведені серед членів закритої підпільної спільноти, показали, що більшість кіберзлочинців заробляють від 1 000 до 3 000 доларів США на місяць, а лише 20 % заробляють значно більшу суму в розмірі $ 20 000 на місяць та більше [4].

З метою здійснення кримінологічної характеристики злочинців у сфері інформаційних технологій науковцями було проведене дослідження з використанням джерел, що є у відкритому доступі в мережі Інтернет стосовно злочинців, які розшукуються за даними Федерального бюро розслідування США [5]. Повний перелік осіб, що складається із 42 підозрюваних, які розшукуються ФБР за підозрою у вчиненні кіберзлочинів, зазначається на відповідному сайті «Найрозшукуваніші злочинці» [5]. За результатами проведеного дослідження виявлені соціально значимі ознаки міжнародного кіберзлочинця. Так, за критерієм віку встановлено, що більшість осіб (60 %), які перебувають у федеральному та міжнародному розшуку, віком від 20 до 35 років, за статевою ознакою досліджувані підозрювані у кіберзлочинах – чоловіки [5].

Варто відмітити, що кіберзлочинці, враховуючи досвід США, належать до категорії особливо небезпечних злочинців, які завдають значну матеріальну шкоду державі, підприємствам, установам, організаціям, інформаційній безпеці. Крім того, у списку відсутні безпосередньо громадяни США [5]. Тому здійснити об'єктивні висновки за територіальними ознаками особистості кіберзлочинців досить складно. Однак, посилаючись на вказані дані, все ж таки можна з певною ймовірністю підтвердити той факт, що більшість злочинців є громадянами держав, в яких присутній низький рівень протидії кіберзлочинам, це – держави Середнього, Далекого Сходу (Пакистан, Індія, Іран, Сирія, В'єтнам тощо). Крім того, важливими є політичні детермінанти, зокрема ставлення урядів окремих держав до цього негативного явища, що зумовило велику кількість підозрюваних у кіберзлочинах з Північної Кореї та Китаю.

Використовуючи міжнародний досвід, було проведено й аналіз та вивчення статистики щодо осіб, які вчиняють кримінальні правопорушення у сфері інформаційних технологій, в Україні. Дослідження проводилося стосовно осіб, яким оголошено про підозру за вчинення кримінальних правопорушень, передбачених чч. 3, 4 ст. 190 КК України [6]. Встановлено, що впродовж 2020 року підрозділами Департаменту кіберполіції Національної поліції України розкрито шахрайств, вчинених шляхом незаконних операцій з використанням електронно-обчислювальної техніки, за 2 012 кримінальними провадженнями, оголошено про підозру 321 особі.

Аналіз даних дав змогу визначити тенденції злочинності у сфері інформаційних технологій за статевою ознакою. Так, 72 % кримінальних проваджень відкриті стосовно чоловіків та 23 % – щодо жінок. Отже, встановлено, що вказана категорія кіберзлочину вчиняється переважно чоловіками, однак існує відсоток і жінок. Крім того, доцільно додати ще один критеріq – кримінальні правопорушення, що вчинені за співучастю особами чоловічо] та жіночо] статі (8 %).

Кібершахрайство має безпосереднє відношення до сегмента інформаційних технологій (IT). А згідно з даними «зарплатного опитування DOU» жінок, які працевлаштовані або перебувають у статусі вільного працівника у сфері інформаційних технологій станом на 2020 рік, лише 20 % [9]. Зазначені дані вказують на рівень залученості жінок у технічні сфери, що тотожно навчанню у технічних закладах вищої освіти або технічній підтримці певного державного і приватного підприємства. Однак, згідно з тими самими результатами вищезазначеного опитування, тенденція збільшення з кожним роком кількості осіб жіночої статі у сфері IT становить у середньому 2 %. Так, 2011 р. частка жінок із вказаними інтересами становила лише 7 % [2].

Розглядаючи соціально-демографічні показники особи, що вчиняє кримінальні правопорушення у сфері інформаційних технологій, варто почати з віку таких осіб. Аналізуючи статистику Офісу Генерального прокурора, потрібно відмітити, що відповідні кримінальні правопорушення вчиняли громадяни віком від 17 до 48 років, тобто від підлітків до осіб старшого віку [7]. Крім того, виявлено факт, що більший відсоток становлять особи у віковому діапазоні від 20 до 35 років, що співпадає з наведеним вище дослідженням стосовно осіб, які розшукуються ФБР США за підозрою у вчиненні кіберзлочинів. З досліджуваної категорії підозрюваних осіб лише 26 % мали одну чи більше вищих освіт, 21 % – особи, що мали середньо-спеціальну освіту. Більшість кібершахраїв мали повну середню освіту, однак це аж ніяк не означає, що українська шкільна програма містить основи щодо скоєння шахрайств з використанням комп'ютерних мереж. Посилаючись на вказаний вище факт, доцільно зробити висновок, що особою кіберзлочинця вказаної категорії здебільшого є людина, яка самостійно отримує або вже здобула освіту у сфері високих інформаційних технологій (комп'ютерної безпеки, програмування, сучасних тенденції розвитку комп'ютерних мереж) поза будь-яким закладом освіти, без педагогічної допомоги.

Щодо національної приналежності, варто зазначити, що переважна більшість кримінальних правопорушень, що вчиняються у сфері інформаційних технологій, скоюється саме українськими громадянами. Лише невеликий відсоток припадає на іноземців. Крім того, у більшості випадків особи вчиняють кримінальні правопорушення за місцем свого проживання (71 %).

Як відмічають науковці, вказані соціально-демографічні ознаки кібершахраїв являють собою лише зовнішню характеристику. Для уявлення про внутрішній світ осіб, що вчинили кримінальне правопорушення, необхідне вивчення їхніх особистісних особливостей. До цих властивостей особистості належать спрямованість, риси характеру, моральні якості, знання, навички, звички, рівень особистої культури тощо. Морально-психологічні якості кібершахраїв у цілому є ідентичними характеристикам шахраїв загальнокримінальної спрямованості [2].

Найбільш притаманними психологічними особливостями шахраїв, за даними сучасних досліджень, є певні мотиви кримінально протиправної поведінки: жага наживи, жадібність, прагнення придбати матеріальні блага і схильність до легкого

життя, більш високий рівень інтелекту (зокрема, порівняно з іншими категоріями злочинців), вміння швидко пристосовуватися до сучасних умов життя, холоднокровність, розважливість, здатність володіти собою, вміння зрозуміти психологію іншої людини і викликати до себе довіру, демонстрація співчуття і співпереживання, акторські здібності, спостережливість, розкутість поведінки, готовність використовувати обман, прагнення до паразитизму, моральна розбещеність, лицемірство, нахабність і грубість, володіння прийомами психологічного впливу на іншу людину тощо [10].

Проте вважаємо, що злочинність у сфері інформаційних технологій є найбільш суспільно небезпечним видом злочинності, де поняття обману та зловживання довірою видозмінилося. Сучасний злочинець може не мати акторських здібностей, вдало брехати і взагалі може не показувати свою поведінку.

Провідне місце серед стійких психологічних особливостей особистості займають мотиви злочинців, властиві прагнення до самоствердження на соціально-психологічному рівні (пов'язано з потребою домогтися визнання з боку найближчого оточення – сім'ї, друзів, знайомих, колег по роботі) і на індивідуальному рівні (пов'язано з бажанням підвищити самооцінку і посилити самоповагу шляхом здійснення вчинків, що сприяють, на думку особистості, подоланню будь-яких психологічних слабкостей). Не менш типовими для кібершахраїв є ігрові мотиви, властиві особам, які скоюють злочини не тільки і не стільки з метою отримання матеріальної вигоди, а скільки заради гри та ризику, для отримання гострих відчуттів. Досить яскраво ці мотиви виявляються в ситуаціях, в яких здійснюється інтелектуальне протиборство і змагання в спритності, де потрібні кмітливість, уміння максимально використовувати сприятливі обставини і швидко приймати рішення [2].

Висновки. Отже, розглянувши наукові праці та дані офіційної статистики, можна сформулювати типовий кримінологічний портрет особи, що вчиняє кримінальні правопорушення у сфері інформаційних технологій:

– більшість підозрюваних за кримінальні правопорушення у сфері інформаційних технологій, які перебувають у міжнародному розшуку, – це чоловіки віком 20–35 років, значна кількість таких злочинців є громадянами держав, в яких присутній низький рівень протидії кіберзлочинам (країни Середнього, Далекого Сходу);

– більшість громадян України, які були підозрюваними за вчинення кримінальних правопорушень у сфері інформаційних технологій, також були особами чоловічої статі, але кримінальні провадження за кібершахрайство відкривались також і щодо жінок та за співучастю особами чоловічої та жіночої статі;

– більше половини підозрюваних злочинців мали вищу освіту, інші мали середньо-спеціальну та середню освіту;

– більшість кібершахраїв самостійно отримують освіту та досвід у сфері високих інформаційних технологій (комп'ютерної безпеки, програмування тощо) поза закладом освіти, без педагогічної допомоги, це зумовлює, що особи кіберзлочинців здебільшого мають спеціальні технічні знання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Харків, 2016. С. 20.

2. Лефтеров Л. В. Кримінологічна характеристика осіб, підозрюваних у кіберзлочинах. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2018. № 35, том 2. С. 65–68. URL: http://vestnik-pravo.mgu.od.ua/archive/juspradenc35/part_2/18.pdf

3. Who Are Cyber Criminals? Academic Programs & Resources. Information Security & Assurance by Norwich University Online. February 13th, 2017. URL: https://online.norwich.edu/academic-programs/masters/information-security-assurance/resources/articles/who-are-cyber-criminals Profiling the Cybercriminal; URL: https://www.sbs.ox.ac.uk/ cybersecurity-capacity/content/profiling-cybercriminal

4. Barysevich A. Inside the Mind of Cybercriminals. URL: https:// www.recordedfuture.com/cyber-criminal-profiling/

5. Cyber's Most Wanted. URL: https://www.fbi.gov/wanted/cyber

6. Кримінальний кодекс України: Закон від 5 квітня 2001 року № 2341-III // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

7. Про осіб, які вчинили кримінальні правопорушення / офіційний сайт Офісу Генерального прокурора. URL: https://gp.gov.ua/ua/posts/pro-osib-yaki-vchinili-kriminalni-pravoporushennya-2 (дата звернення: 06.06.2022).

8. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: наказ МВС України від 12 жовт. 2009 року № 436.

9. Женщины в IT: портрет, планы, мотивация. URL: https://dou.ua/lenta/articles/it-woman/

10. Борисова С. Е. Психологические особенности лиц, совершивших мошенничество, и их учет при расследовании преступлений. *Прикладная юридическая психология.* 2008. № 1. С. 108–115.

REFERENCES

1. Kravtsova M. O. Cybercrime: criminological characteristics and prevention of internal affairs: author's ref. dis. for science. degree of Cand. jurid. Science: special. 12.00.08 "Criminal law and criminology; criminal executive law". Kharkiv, 2016. P. 20.

2. Lefterov L. V. Criminological characteristics of persons suspected of cybercrime. *Scientific Bulletin of the International Humanities University. Ser.: Jurisprudence.* 2018. № 35, Volume 2. Pp. 65–68. URL: http://vestnik-pravo.mgu.od.ua/archive/juspradenc35/part_2/18.pdf

3. Who Are Cyber Criminals? Academic Programs & Resources. Information Security & Assurance by Norwich University Online. February 13th, 2017. URL:

https://online.norwich.edu/academic-programs/masters/information-security-assurance/resources/articles/who-are-cyber-criminalsProfiling the Cybercriminal; URL: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/profiling-cybercriminal

4. Barysevich A. Inside the Mind of Cybercriminals. URL: https://www.recordedfuture.com/cyber-criminal-profiling/

5. Cyber's Most Wanted. URL: https://www.fbi.gov/wanted/cyber

6. Criminal Code of Ukraine: Law of April 5, 2001 № 2341-III // Database "Legislation of Ukraine" / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

7. On persons who have committed criminal offenses: the official website of the Office of the Prosecutor General. URL: https://gp.gov.ua/en/posts/pro-osib-yaki-vchinili-kriminalni-pravoporushennya-2 (access date: 06.06.2022).

8. On approval of the Regulations on the Integrated Information Search System of the Bodies of Internal Affairs of Ukraine: Order of the Ministry of Internal Affairs of Ukraine of October 12. 2009 № 436.

9. Women in IT: portrait, plans, motivation. URL: https: dou.ua/lenta/articles/it-woman/

10. Borysova C. E. Psychological features of perpetrators of fraud and their consideration in the investigation of crimes. *Applied legal psychology*. 2008. № 1. S. 108–115.

O. Bodunova. Criminological characteristics of a person committing criminal offenses in the field of information technologies

The article describes a person who commits criminal offenses in the field of information technology. The relevance of the chosen research topic is due to the fact that the rapid development of technological progress in recent years has led to the acceleration of various processes, both state and non-state. At the same time, information technology has been actively used by criminals for criminally illegal purposes. This speeds up the commission of criminal offenses and also allows criminals to remain "unnoticed" in the eyes of law enforcement agencies for a long time.

In addition, criminal offenses committed in the field of information technology are characterized by increased public danger, as they relate to other areas, including property, national security, public safety and more. The share of the above-mentioned criminal offenses committed in these areas is 2–3 times higher than 10 years ago. In this regard, one of the most pressing issues today is the development of an updated model of crime prevention in the field of information technology, as the latter is very quickly and actively transformed, criminals use new methods of committing criminal offenses unknown to law enforcement.

Such criminological analysis of criminal offenses committed with the use of information technology, and the development of effective ways and directions to prevent them is impossible without taking into account the typical personal characteristics of persons who directly commit cybercrime. That is why it is expedient and urgent to study the characteristics of a person who commits criminal offenses in the field of information technology.

The aim of the article is to study the typical features and characteristics of persons who commit criminal offenses in the field of information technology in order to form an effective model for crime prevention in this area.

Research methods: in the process of writing a scientific article the following methods were used: dialectical – to learn about individual processes, phenomena, statistical – during the analysis of official data on persons who have committed a criminal offense in the field of information technology; systemic – when considering the types of cybercriminals, etc.

Considering scientific works and official statistics, a typical criminological portrait of a person committing criminal offenses in the field of information technology is formulated.

Keywords: *cybercriminals, information technology crime, criminal offense, socio-demographic characteristics, moral and psychological characteristics, prevention.*

Стаття надійшла до редколегії 10 червня 2022 року