УДК 343.3

Піцик Ю. М.,
секретар
Кваліфікаційно-дисциплінарної комісії прокурорів

АНАЛІЗ ОСОБИСТОСТІ КІБЕРЗЛОЧИНЦЯ, ЯКИЙ ВЧИНЯЄ ЗЛОЧИНИ ПРОТИ ВЛАСНОСТІ У КІБЕРПРОСТОРІ

Анотація. В статті надано характеристику особистості кіберзлочинця. Виявлено, описано та проаналізовано соціально-демографічні, кримінально-правові та морально-психологічні риси осіб, засуджених за вчинення кіберзлочинів. Зроблено висновок про те, що заходи протидії кіберзлочинності повністю втрачають свій сенс без урахування особливостей особистості конкретного правопорушника. Виявлення сталих та найпоширеніших рис комп'ютерного злочинця дасть можливість обрати найбільш ефективні способи попередження нових злочинних проявів як з боку конкретної особи, так і з боку невизначеного кола осіб на яких ці заходи спрямовуються.

Ключові слова: кіберзлочинність, кіберзлочинець, особистість злочинця, ознаки кіберзлочинця, мотивація кіберзлочинця.

Постановка проблеми. На сучаному етапі розвитку суспільства та в умовах стрімкого поширення комп'ютеризації у всіх сферах життєдіяльності, інформаційно–телекомунікаційні мережі виступають засобом вчинення злочинів, що охоплюються загальним поняттям кіберзлочинність. Внаслідок цього особлива увага повинна приділятися особистості кіберзлочинця, що і обумовлює актуальнісь надання її кримінологічної характеристики [1, с. 1].

У той же час доцільно вказати на збільшення кількості злочинів проти власності, які вчиняються у кіберпросторі та поширення таких злочинів у світі, зокрема й злочинців, які мають українське коріння. Зокрема, як повідомила «Німецька хвиля» з посиланням на міністерство юстиції США, у 2017 році американські правоохоронці припинили діяльність злочинного угруповання Infraud, яке у 2010 році створив українець Святослав Бондаренко. Так, група кіберзлочинців діяла під гаслом «In Fraud We Trust», тобто «Ми віримо в шахрайство». Зловмисники створили розгалужену й добре організовану мережу, що протизаконним шляхом отримувала особисті дані інтернет–користувачів, у тому числі ті, що надавали доступ до банківських та електронних рахунків. Як вважають слідчі, члени угруповання намагалися отримати дані про 4,3 мільйона кредитних карток та банківських рахунків.

За час існування угруповання злочинці завдали своїми діями збитків на понад 530 мільйонів доларів, наголосили в міністерстві юстиції США. Наразі слідчі вважають причетними до злочинного угруповання загалом 36 осіб. 13 членів кібербанди вже заарештували. Арешти проводилися в США, Австралії, Великобританії, Франції, Італії, Косові, Сербії та Албанії, зазначається в повідомленні [2].

Аналіз останніх досліджень і публікацій. Проблему кіберзлочинності на теренах України та у зарубіжній науці досліджували такі автори, як В. Дзюндзюк, Б. Дзюндзюк, М. МакГуайр, С. Даулинг, С. Фафінські та ін.

Побудувати портрет комп'ютерного злочинця пробували багато вітчизняні вчені, але єдиної точки зору немає, що пов'язано з різноманітністю кіберзлочинності, тому метою статті є проведення аналізу та надання кримінологічної характеристики особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі.

Виклад основного матеріалу дослідження. При визначенні структури особистості злочинця, кримінологи виділяють різні ознаки, які можна об'єднати в такі групи: соціально–демографічні, кримінально–правові та морально– психологічні ознаки [3, с. 10]. Соціально–демографічні ознаки дають інтегроване уявлення про особу злочинця та допомагають встановити її функціональний зв'язок із вчиненим злочином, розкривають характеристику соціального статусу і свідчать про його вплив на злочинця [4, с. 89].

Аналіз спеціальної літератури показав, що злочини у сфері використання комп'ютерної техніки та інформаційно–телекомунікаційних мереж вчиняють переважно чоловіки (87,5 %), на жінок припадає лише 12,5 %. Що стосується вікових груп, то аналіз їх розподілу за рівнем кримінальної активності показав, що найбільш активною є група осіб віком від 30 до 50 років, частка якої становить 36,2 % засуджених, на другому місці група осіб віком від 18 до 25 років (34,3 %), на третьому – особи віком від 25 до 30 років (23,1 %), на останньому – особи віком від 16 до 18 років (1,1 %). Наведені дані в цілому співпадають зі світовою практикою. Зокрема, проведені дослідження в Австралії, Канаді, Німеччині, США вказують на те, що найбільш активний віковий період в якому вчиняються комп'ютерні злочини становить вік від 15 до 35 років [5, с. 9].

Характеристика особистості злочинця, здатного вчинити кіберзлочини проти власності, є важливою частиною розуміння самого явища кіберзлочинності. Отримані дані допоможуть виділити приблизне коло осіб, які потребують додаткового контролю з боку правоохоронних органів, що полегшить пошук винних і попередження нових злочинів проти власності, які вчиняються у кіберпросторі. Дане дослідження представляє особливий інтерес, якщо врахувати, що Європол опублікував звіт «Оцінка загрози організованої злочинності в ЄС», в якому кіберзлочинці з країн пострадянського простору займають перше місце в Європі за кількістю вихідних комп'ютерних атак [6].

Оскільки в кіберпросторі існує можливість вчинення різних злочинів проти власності, що вимагають наявності різних навичок і знань, то і кіберзлочинців ділять на різні групи, тому що вони мають різні особистісні характеристики. Так, виділяють:

1) корисливих злочинців;

2) осіб які вчинили кіберзлочини проти власності через недбалість;

3) хакерів;

4) кракерів (комп'ютерних хуліганів) тощо [7, с. 27–30].

Окремі дослідники ділять осіб, які вчинили кіберзлочини, на три групи:

1) «фанатики» – особи, відмінною рисою яких є стійке поєднання професіоналізму в сфері комп'ютерної техніки і програмування з елементами фанатизму (хакери);

2) «психічно хворі» – особи, які страждають на такі психічні захворювання, як інформаційна хвороба або комп'ютерна фобія;

3) «профі» – професійні комп'ютерні злочинці з яскраво вираженими корисливими цілями [8, с. 30].

Аналізуючи таке розмаїття видів кіберзлочинців, можна виявити одну особливість: майже всі вчені так чи інакше виділяють дві самостійні групи кіберзлочинців: хакерів і корисливих злочинців. Якщо врахувати, що ці дві групи одна одну не виключають, то серед корисливих кіберзлочинців можна зустріти як хакерів, так і звичайних користолюбців–шахраїв. Також серед хакерів можна зустріти як корисливих хакерів, так і навпаки, некорисливих (наприклад, рухомих хуліганськими мотивами).

Вбачається, що доцільно проаналізувати особистість саме корисливого кіберзлочинця, оскільки переважна більшість кіберзлочинів проти власності – корисливі.

Впершу чергу требі з'ясувати вікові характеристики такого злочинця. При порівнянні даних про вік кіберзлочинця з даними про вік злочинця, що вчиняє аналогічні злочини без використання комп'ютера і кіберпростору, виявляється своя специфіка. Так, якщо середній вік шахрая, який вчиняє злочин в матеріальному світі (без допомоги комп'ютерної техніки), коливається від 23 до 39 років, то середній вік кібершахрая варіюється від 18 до 26 років. При цьому якщо частка неповнолітніх, які вчиняють кіберзлочини проти власності, становить 30%, то в матеріальному світі біля 10%. Зокрема, в структурі злочинності неповнолітніх домінують злочини проти власності, які складають 81 % всіх злочинів неповнолітніх, що підкреслює її переважно корисливу спрямованість. Серед них переважають крадіжки – 67 %, грабежі – 9 %, шахрайства і розбої – близько 2 %.

Також при порівнянні даних про вік кіберзлочинця з початку 2000–х років до сьогодні простежується тенденція щодо омолодження кіберзлочинця: якщо середній вік у 2002 році становив приблизно 30 років, то сьогодні – тільки 24 роки. Така тенденція дуже небезпечна, оскільки може привести до того, що середній вік кіберзлочинця знизиться нижче планки повноліття, і кіберзлочинність стане ювенальною.

Звісно ж омолодження особистості кіберзлочинця пов'язано з омолодженням особистості користувача мережі «Інтернет». Як вірно вказується в спеціальній літературі, найбільш активна у оволодінні мережею Інтернет є молодь, яка складає 48% від усіх користувачів [9, с. 4]. Середній вік користувачів мережі «Інтернет» у 2004–2006 роках становив 30 років, а сьогодні знаходиться на позначці від 14 до 24 років.

Таким чином проведений аналіз показав, что вік кіберзлочинця коливається від 15 до 45 років, а соціальне становище в суспільстві – від школяра і студента до відповідального співробітника державної установи або фірми.

Певні зміни виявляються при порівнянні даних про стать злочинця, що вчиняє кіберзлочини проти власності, з даними про злочинців, які вчиняють аналогічні злочини в матеріальному світі. Так, якщо співвідношення чоловік / жінка в традиційних злочинах становить 70% на 30%, то в кіберзлочини частка чоловіків–злочинців становить вже 97%, а жінок – лише 3%. За статистичними даними більшість кіберзлочинців проти власності (79%) – це шахрайства, які, як правило, вчиняються чоловіками (94%) і лише в рідкісних випадках жінками (6%). У той же час якщо взяти інший, менш поширений з кіберзлочинів, наприклад, привласнення і розтрату, то частка чоловіків серед загального числа злочинців знизиться до 50% [1, с. 5].

Як правило, кіберзлочини вчиняються особами, які офіційно не перебувають у шлюбі. Кількість неодружених осіб із загального числа кіберзлочинців становить 70%, в той час як одружених – 30%. Дане співвідношення справедливо для злочинців, які вчиняють як злочини проти власності, так і злочини в сфері економічної діяльності. Звісно ж, що це пов'язано в першу чергу з середнім віком кіберзлочинця, а також з певними суб'єктивними факторами: сімейні люди рідше вчиняють злочини, ніж самотні, побоюючись, що це негативно позначиться на їх близьких.

Аналізуючи судову практику у справах про злочини, що вчиняються з використанням високих технологій та кіберпростору, можна прийти до висновку, що дана група злочинів відноситься до групи високоінтелектуальних злочинів. Майже третина (28%) всіх кіберзлочинців мають вищу освіту. При цьому 14% кіберзлочинців мають незакінчену вищу освіту. У більшості випадків на момент вчинення злочину вони були студентами вищих навчальних закладів. 32% кіберзлочинців мають середню спеціальну освіту, 21,5% – середню загальну і лише 4,5% – неповну середню освіту. Досить великий відсоток осіб, що мають технічні спеціальності «Прикладна інформатика», «Інформаційні системи і технології», «Програмна інженерія», «Інформаційна безпека» тощо, – приблизно 33%. Кіберзлочинці саме цієї групи часто використовують шкідливі програми і віруси. Вони знають принципи роботи інформаційно-телекомунікаційних мереж, знають їх уразливості тому й користуються цим [1, с. 6]. Зокрема 38,2% злочинців, які вчиняли злочини в мережі Інтернет, мали вищу освіту або навчалися у вищих навчальних закладах, 25,7% з яких – на технічних спеціальностях. 39,3% кіберзлочинців – це учні вищих навчальних закладів або технікумів. 78% кіберзлочинців мають вищу освіту.

Як показує судова практика, 51% осіб, які вчинили кіберзлочини, не мають постійного місця роботи. Як правило, згадані особи вчиняють шахрайства. Серед решти 49% більшу частину займають менеджери нижчої та середньої ланки, рідше зустрічаються посадові особи і програмісти. 31,3% осіб, які вчинили злочини в мережі «Інтернет», мали постійне місце роботи.

Як правило, кіберзлочини проти власності вчиняються в великих містах. Звісно ж, що це пов'язано з рядом факторів: по–перше, в великих містах розвинені інформаційно–телекомунікаційні технології та є доступ до безлімітного «Інтернету»; по–друге, в таких містах більше населення, що безпосередньо позначається на статистиці. Однак у судовій практиці зустрічалися випадки вчинення кіберзлочинів в невеликих селищах, селах, в яких також було проведено «Інтернет».

З аналізу судової практики видно, що 78% осіб, визнаних винними у вчиненні кіберзлочинів, раніше не притягувалися до кримінальної відповідальності, а лише 22% мали непогашену чи не зняту судимість. При цьому приблизно 50% з них мали судимість за вчинення злочинів проти власності, 33% мали судимість за злочини у сфері комп'ютерної інформації, а решта 16% мали судимість за інші злочини [1, с. 7].

Висновки. Підводячі певні підсумки доцільно вказати, що при вивченні особистості кіберзлочинця потрібно зосередитися на його мотивації. Для більшості злочинів проти власності, які вчиняються у кіберпросторі метою є заволодіння чужим майном. Проте, сюди можна віднести і користь, і помсту, і потребу у самоствердженні тощо. Досліджуючи мотивацію кіберзлочинців, необхідно використовувати усталені поняття, а не шукати якихось специфічних мотивів. Слід наголосити на тому, що особливість кіберзлочинності більшою мірою полягає не в мотивах вчинення злочинів, а в особливостях їх реалізації,

обумовлених специфікою середовища та засобів їх вчинення. Однак, не можна недооцінювати мотив даного виду злочину, оскільки його правильне встановлення дозволить не лише уникнути помилок при кваліфікації, а й успішно реалізувати принципи справедливості та невідворотності покарання.

Проведений аналіз особистості кіберзлочинця дає підстави скласти кримінологічний портрет особи, що вчиняє злочини проти власності у кіберпросторі, це: чоловік, який має середній вік 24 роки, раніше не судимий, неодружений, не має постійного місця роботи, житель великого міста, з розвиненою інформаційно-телекомунікаційною інфраструктурою, випускник або учень вищого навчального закладу, має високий навик роботи з комп'ютерною технікою, інформаційно-телекомунікаційними мережами і (або) шкідливим програмним забезпеченням, усвідомлює протиправність своїх дій і рухомий корисливим мотивом.

Відповідно, нами вбачається за доцільне виділити два основних типи кіберзлочинців, які вчиняють злочини проти власності у кіберпросторі:

1. Перший тип (традиційні кіберзлочинці), тобто особи, які вчиняють традиційні злочини (шахрайство, привласнення, розтрату, вимагання) з використанням загальнодоступних ресурсів і можливостей кіберпростору (таких як електронна пошта або соціальні мережі).

2. Другий тип (хакери), тобто особи, які вчиняють кіберзлочини проти власності за допомогою неправомірного доступу до комп'ютерної інформації або з використанням шкідливого програмного забезпечення в кіберпросторі (вірусів, троянських програм, DDoS–програм тощо).

Пропоновані типи кіберзлочинців багато в чому відрізняються один від одного. Так, кіберзлочинці першого типу, як правило, старші і досвідченіші хакерів – саме в цій групі кіберзлочинців найбільша кількість осіб, які мають судимість. Хакери, навпаки, як правило, молодше і є випускниками або учнями вищих навчальних закладів технічного спрямування або спеціальних технікумів і коледжів.

Кіберзлочинці першого типу вчиняють традиційні злочини, тобто ті, які вчиняються і без використання кіберпростору (шахрайства, вимагання). Такі кіберзлочинці при вчиненні злочинів не використовують складні шкідливі програми і віруси, а користуються можливостями кіберпростору, які є в загальному доступі: шахрайство шляхом обману вони вчиняють за допомогою соціальних мереж, вимагання – через електронну пошту і так далі. Кіберзлочинці другого типу при вчиненні злочинів користуються технічними можливостями кіберпростору, «зламують» електронні поштові скриньки, мобільні телефони, банківські онлайн–рахунки та електронні гаманці. Такі кіберзлочинці добре розбираються в складних комп'ютерних програмах, знають принципи роботи інформаційно–телекомунікаційних мереж і вміють «користуватися» вірусами і іншим шкідливим програмним забезпеченням.

Таким чином підсумовуючи, можна зробити висновок про те, що заходи протидії кіберзлочинності повністю втрачають свій сенс без урахування особливостей особистості конкретного злочинця. Виявлення сталих та найпоширеніших рис кіберзлочинця дасть можливість обрати найбільш ефективні способи попередження нових злочинних проявів як з боку конкретної особи, так і з боку невизначеного кола осіб на які ці заходи спрямовуються.

Література:

1. Кравцова М. О. Сучасний кіберзлочинець: кримінологічна характеристика особистості / М.О. Кравцова. – Х., 2015. – 8 с.
2. У США викрили створену українцем міжнародну мережу кіберзлочинців [Електронний ресурс]. – Режим доступу: https://zaxid.net/u_ssha_vikrili_stvorenu_ukrayintsem_mizhnarodnu_merezhu_kiberzlochintsiv_n1448553.
3. Голіна В.В. Попередження тяжких насильницьких злочинів проти життя, здоров'я особи / В.В. Голіна. – Х.: Рубікон, 1997. – 52 с.
4. Коган В.М. Значение социально-демографических факторов для изучения причин преступности / В.М. Коган // Вопросы борьбы с преступностью. – 1975. – Вып. 22. – С. 88– 94 с.
5. Біленчук П.Д. Портрет комп'ютерного злочинця: навч. посібник / П.Д. Біленчук, О.І.Котляревський. – К.: 1997. – 48 с.
6. Socta 2013. EU Serious and Organised Crime Threat Assessment. [Електронний ресурс]. – Режим доступу: https://www.europol.europa.eu/sites/ default/files/publications/socta2013.pdf.
7. Батурин Ю.М. Право и политика в компьютерном круге. М., – 1987. – С. 27–34.
8. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. М., – 1996. – С. 31–36.
9. Гузеева О.С. Предупреждение размещения информации, способствующей распространению наркотических средств, в российском сегменте сети Интернет (криминологические и уголовно–правовые проблемы). автореф. дис. … канд. юрид. наук. М., – 2008. – С. 4.

Пицик Ю. М. Анализ личности киберпреступника, совершающего преступления против собственности в киберпространстве

Аннотация. В статье охарактеризованы личности киберпреступников. Выявлено, описано и проанализировано социально-демографические, уголовно-правовые и морально-психологические черты лиц, осужденных за совершение киберпреступлений. Сделан вывод о том, что меры противодействия киберпреступности полностью теряют свой смысл без учета особенностей личности конкретного правонарушителя. Выявление устойчивых и распространенных черт компьютерного преступника даст возможность выбрать наиболее эффективные способы предупреждения новых преступных проявлений как со стороны конкретного лица, так и со стороны неопределенного круга лиц на которых эти мероприятия направлены.

Ключевые слова: киберпреступность, киберпреступник, личность преступника, признаки киберпреступника, мотивация киберпреступников.

Pitsyk Yu. Analysis of the identity of cybercriminals who commit crimes against property in cyberspace

Summary. The characteristic personality cybercriminal. Identified, described and analyzed sociodemographic, criminal and moral-psychological characteristics of persons convicted of committing cybercrimes. It is concluded that measures to combat cybercrime completely lose their meaning without taking into account the personality characteristics of a particular offender. Identifying the persistent and most common features of a computer offender will enable you to choose the most effective ways of preventing new criminal manifestations both from a particular person and from an uncertain range of people on whom these measures are directed.

Key words: cybercrime, cybercriminal, identity of the offender, characteristics of cybercriminal, motivation of cybercriminal.