УДК 343.1
DOI https://doi.org/10.32782/392266

Тарасенко О. С.,
доктор юридичних наук, доцент,
професор кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ

ХАРАКТЕРИСТИКА ОСІБ ТА ЗЛОЧИННИХ УГРУПОВАНЬ, ЯКІ ВЧИНЯЮТЬ КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ, ПОВ'ЯЗАНІ З ОБІГОМ ПРОТИПРАВНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ

CHARACTERISTICS OF PERSONS AND CRIMINAL GROUPS COMMITTING CRIMINAL OFFENSES RELATED WITH THE CIRCULATION OF ILLEGAL CONTENT ON THE INTERNET

У статті досліджені соціально-демографічні, кримінально-правові та морально-психологічні риси особи злочинця у кримінальних правопорушеннях, пов'язаних з обігом протиправного контенту в мережі Інтернет. Надана характеристика таких осіб з виокремленням тих, які представляють оперативний інтерес, зокрема: які не мають права доступу до певної інформації, але мають зв'язки з нею; співробітники організації, які мають право доступу до інформації у зв'язку із займаною посадою або спеціальними повноваженнями; співробітники організації, які є користувачами та відносяться до персоналу, перебувають у трудових відносинах з власником технічних засобів і визначені для здійснення функцій управління та обслуговування ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Наголошено, що кримінальні правопорушення, пов'язані з обігом протиправного контенту в мережі Інтернет, доцільно поділити на три основні умовні групи: 1) вчиняються у зв'язку з професійною (службовою) діяльністю особи; 2) вчиняються особами з низьким офіційним соціальним статусом (безробітні тощо) з метою незаконного збагачення; 3) вчиняються з особистих (крім користі) мотивів (самоствердження, помста тощо). Констатовано, що використовуючи Інтернет як середовище для протиправної діяльності, організовані групи звертають увагу на можливості, які їм дає мережа обміну інформацією: у будь-якому місці та будь-який час виходити на зв'язок, оперувати практично без обмежень за обсягом текстовою та графічною інформацією забороненого змісту, при цьому зберігаючи анонімність абонента-користувача мережі Інтернет й здійснювати в глобальних масштабах інформаційно-психологічний вплив на людей з метою поширення забороненого контенту. Зосереджено увагу на мережевій та корпоративній моделях організованої групи, що протиставляються між собою. З'ясовано, що злочинці у кримінальних правопорушеннях, пов'язаних з обігом протиправного контенту в мережі Інтернету своїй більшості мислячі, творчі люди, у свідомості і поведінці яких, на жаль, переважають почуття помсти, заздрості і бажання довести своєму оточенню власне лідерство. Головною мотивацією їх вчинків є прагнення збагачення навіть під загрозою кримінального покарання.

Ключові слова: *протиправний контент, Інтернет, особа злочинця, злочинне угрупування.*

The article examines the socio-demographic, criminal law and moral and psychological traits of the offender in criminal offenses related to the circulation of illegal content on the Internet. The characteristics of such persons are given, with the exception of those who are of operational interest, in particular: who do not have the right to access certain information, but have connections with it; employees of the organization who have the right to access information in connection with the position or special powers; Employees of the organization, who are users and belong to the staff, are in an employment relationship with the owner of the technical means and are assigned to perform the functions of management and maintenance of EC (computer), automated systems, computer networks or telecommunications networks. It is emphasized that criminal offenses related to the circulation of illegal content on the Internet should be divided into three main conditional groups: 1) committed in connection with the professional (official) activities of the person; 2) are committed by persons with low official social status (unemployed, etc.) for the purpose of illicit enrichment; 3) are committed for personal (in addition to benefit) motives (self-affirmation, revenge, etc.). It was stated that using the Internet as an environment for illegal activities, organized groups pay attention to the opportunities provided by the network of information exchange: anywhere and at any time to communicate, operate with almost no restrictions on the amount of text and graphics information of prohibited content, while maintaining the anonymity of the subscriber-user of the Internet and to carry out global informational and psychological influence on people in order to disseminate prohibited

content. The focus is on the network and corporate models of the organized group, which oppose each other. It has been found that the majority of criminals in criminal offenses related to the circulation of illegal content on the Internet are thinking, creative people, whose minds and behavior, unfortunately, are dominated by feelings of revenge, envy and the desire to prove their leadership. The main motivation for their actions is the desire to get rich, even under threat of criminal punishment.

Key words: *illegal content, Internet, criminal identity, criminal group.*

Актуальність статті. Існування людини у віртуальному просторі виражається у використанні нею спеціальних програм, технічних засобів, комп'ютерних і телефонних додатків, які спрощують та оптимізують життя людини. Такими засобами є електронна пошта, електронні платіжні системи, кредитні та платіжні картки, записи в електронних книгах, календарі, соціальні та пошукові мережі тощо, внаслідок експлуатації яких незалежно від волі людини в електронній мережі залишаються віртуальні сліди, що генеруються використовуваними людиною електронними пристроями. Стаючи частиною суспільного життя, віртуальний простір стає частиною злочинного світу, де накопичені криміналістикою знання стають недостатніми для виконання завдань кримінального провадження [1, с. 426].

Особу злочинця, який вчиняє кримінальні правопорушення, пов'язані з обігом протиправного контенту в мережі Інтернет, можна охарактеризувати як сукупність найістотніших стійких соціальних властивостей та ознак, а також соціально значущих біопсихологічних особливостей певного індивіда, які об'єктивно реалізуються при їх вчиненні, надаючи вчиненому діянню характер суспільної небезпечності, а винній у його вчиненні особі – властивості суспільної небезпечності, у зв'язку з чим вона є суб'єктом кримінального правопорушення [2, с. 152].

Виклад основного матеріалу. Сьогодні кіберзлочинцям вченими надаються неоднозначні соціально-психологічні характеристики, які засновані на узагальнених емпіричних даних, оскільки сам предмет розгляду недостатньо вивчений з причин специфічності й складності цих кримінальних правопорушень [3, с. 78]. Як зазначає Д. С. Азаров, на жаль, вітчизняна кримінологія не має у своєму арсеналі даних узагальнюючого характеру щодо особи цих злочинців, майже відсутні публікації з цього приводу. А окремі характеристики «комп'ютерного злочинця» (як то: вік – 24–25 років (середній вік – 30 років); за освітою – інженер в галузі електроніки і математики, займає відповідальну посаду (віце-президент компанії, фінансові керівники, скарбники, вкладники капіталів тощо); можуть не мати ніякої технічної освіти; не мають кримінального минулого; більшість становлять чоловіки, але можуть зустрічатися й жінки; загалом це яскрава, думаюча, творча особа, професіонал своєї справи, готовий прийняти технічний виклик, бажаний працівник [4, с. 15–16], як справедливо зауважує вчений, є поверхневими, суперечливими та емпірично необґрунтованими [5, с. 132].

Аналіз даних щодо засуджених осіб в Україні показав, що кіберзлочини вчиняються переважно чоловіками (90,8%), на долю жінок припадає лише 9,2% кримінальних правопорушень. Такий статевий розподіл кіберзлочинців обумовлений не лише традиційно низькою у порівнянні з чоловіками кримінальною активністю жінок, але й з специфікою даного виду кримінальних правопорушень. Професійне з технічної точки зору вчинення кіберзлочинів жінками практично не спостерігається, оскільки вони менш представлені серед технічних спеціальностей. Вчинення професійних кіберзлочинів особами жіночої статі обумовлене їх соціальним статусом, пов'язаним з професійною діяльністю, здійснення якої передбачає використання комп'ютерних технологій [6, с. 385–386].

Вік злочинця вказує не лише на рівень біологічного, а й соціального розвитку людини, на відповідний стан і зміни особистості людини. Здійснюючи перехід з одного вікового ступеня на інший, людина постійно взаємодіє з соціальним середовищем, отримує і накопичує життєвий досвід [7, с. 54]. Аналіз віку злочинця дозволяє, своєю чергою, виявити найбільш кримінально активні вікові групи населення.

Характерним на відміну від загальнокримінальної злочинності є відсутність серед засуджених осіб вікової групи від 65 років і старше. Це обумовлене, передусім, відсутністю у більшості осіб даної вікової групи відповідних навичок роботи з комп'ютерною технікою, а також більшим життєвим досвідом і вищими моральними цінностями.

Аналіз розподілу вікових груп за рівнем кримінальної активності показав, що найбільш активною є група осіб віком від 30 до 50 років, на долю якої припадає 43,1% засуджених за кіберзлочини осіб. На другому місці знаходиться група осіб віком від 18 до 25 років (27,5%), на третьому − особи віком від 25 до 30 років (24%), на четвертому − особи віком від 50 до 65 років (4,7%), а на останньому місці, як вже зазначалося, знаходиться група осіб віком від 16 до 18 років (0,7%).

Таким чином, хоча більше половини (51,5%) кіберзлочинів вчиняються особами віком від 18 до 30 років, кримінальна активність відносно даного виду злочинів корелює з соціальною активністю населення. Також необхідно відмітити поступове падіння кримінальної активності вікових груп 18–25 років та 50−65 років: якщо у 2015 р. частка перших становила 24%, а других – 8,7%, то у 2020 р. – 17,4% та 2,2%, відповідно. Як видається, така тенденція може бути пояснена інтенсивним розвиток комп'ютерних технологій, що зумовлює, по-перше, необхідність отримання попереднього досвіду мережевої і/або програмістської роботи, та, по-друге, відомі труднощі для осіб поважного віку щодо освоєння вказаних технологій.

Здійснений нами аналіз кримінальних проваджень виявив, що більшість кіберзлочинців неодружені – 58%. Розлучені становлять 14%, а одружені, але такі, що з родиною не живуть, – 16%. На долю одружених припадає 10%, а на осіб, що перебувають у цивільному шлюбі, – 12%. Таким чином, переважна більшість кіберзлочинців – особи, які не мають дружини/чоловіка. Це може бути обумовлено значною частиною серед кіберзлочинців осіб молодого віку, які не встигли завести сім'ю, а також характерною для кіберзлочинців нестабільністю особистості, жагою ризику, авантюризмом тощо, тобто властивостями характеру, які не сприяють зміцненню сімейних відносин.

У ході дослідження встановлено, що загалом для кіберзлочинців на відміну від злочинців, що вчиняють злочини загальнокримінальної спрямованості, характерний високий освітній рівень, вищий рівня освіти населення. Так, переважна кількість кіберзлочинців (48,1% засуджених осіб) – це особи з вищою освітою (з них з повною вищою освітою – 33,9%, з базовою вищою освітою – 14,2%). Другою за поширеністю є група осіб із загальною середньою освітою (30,3%), з яких повну загальну середню освіту мають 25,3% осіб, а базову загальну середню освіту – 5% осіб. Частка осіб з професійно-технічною освітою складає 21,1%. Виявлений один випадок (0,3%) засудження за вчинення кіберзлочину особи з початковою загальною освітою. Осіб без освіти не виявлено.

Таким чином, половина (48,1%) кіберзлочинців мають вищу (зокрема, технічну) освіту, однак факт, що кожен третій злочинець (30,3%) має загальну середню освіту вказує на наступне. З розвитком комп'ютерних технологій та систем комунікації, їх агресивною ескалацією в усі сфери нашої життєдіяльності, все більш поширеним стає вчинення кіберзлочинів не фахівцями-комп'ютерщиками, а звичайними користувачами кібертехнологій. Досягнення у цій сфері уможливили вчинення кіберзлочинів не за допомогою відповідної освіти, багажу знань і навичок, а за допомогою відповідних керівництв та посібників.

Встановлено, що переважна більшість засуджених кіберзлочинців – працездатні особи, які на момент вчинення злочину не працювали і не навчалися (43,7%), та безробітні (2,5%). При цьому потрібно відзначити тенденцію до зростання останніми роками частки саме вказаної категорії осіб.

Загалом розподіл осіб, засуджених за вчинення кіберзлочинів, за родом їхніх занять вказує, що другою за поширеністю є група службовців, на частку яких припадає 17% (з них 1,7% державні службовці). Третьою – робітники (16,1%) та приватні підприємці (11,4%). На п'ятому місці за поширеністю знаходиться група осіб, що навчаються – 7,4% (6,9% складають студенти навчальних закладів, а 0,5% – учні шкіл, ліцеїв, коледжів, гімназій). На шостому місці за поширеністю серед осіб, засуджених за вчинення кіберзлочинів, − працівники господарських товариств (3,3%), а на сьомому – пенсіонери (зокрема, інваліди) (1,1%). Також зустрічаються поодинокі випадки засудження за вчинення кіберзлочинів військовослужбовців, лікарів, фармацевтів тощо [8].

Отже, аналіз соціального статусу кіберзлочинця дозволяє підтвердити справедливість висновку, що кримінальні правопорушення, пов'язані

з обігом протиправного контенту в мережі Інтернет, доцільно поділити на три основні умовні групи: 1) вчиняються у зв'язку з професійною (службовою) діяльністю особи; 2) вчиняються особами з низьким офіційним соціальним статусом (безробітні тощо) з метою незаконного збагачення; 3) вчиняються з особистих (крім корисні) мотивів (самоствердження, помста тощо).

Відповідно до даних Міністерства юстиції України, серед осіб, засуджених за вчинення кіберзлочинів, 5,1% фактично раніше вчиняли кримінальні протиправні діяння. Однак, кримінально-правового рецидиву не мають, оскільки вони були звільнені від кримінальної відповідальності (0,5%), визнані такими, що не мають судимості (1,9%), або судимість погашена чи знята (2,7%).

Водночас 5,8% осіб, засуджених за вчинення кіберзлочинів, мають незняту і непогашену судимість. З них 5% мають одну та 0,8% − дві незняті й непогашені судимості. При цьому частка осіб, які мають незняту і непогашену судимість, є відносно стабільною.

Дослідження матеріалів кримінальних проваджень також вказує на корисливий характер кримінальної орієнтації кіберзлочинців з огляду на їх попередню злочинну діяльність. Те, що більшість осіб, які раніше засуджувались, – засуджувалися за вчинення кримінальних правопорушень корисливої спрямованості при тому, що переважна більшість засуджених кіберзлочинців – працездатні особи, які на момент вчинення кримінального правопорушення не працювали і не навчалися, свідчить про глибоку та стійку кримінальну спрямованість особистості злочинців цієї групи та характерну деформацію ціннісно-орієнтаційної сфери.

Досліджуючи особистість злочинця, не можна не враховувати значення індивідуально-психологічних особливостей особистості у разі вчинення конкретного злочину, оскільки в цьому випадку вони можуть визначати поведінку особистості. Пізнання ж особливостей внутрішнього світу злочинців, зокрема їх моральних якостей, потребує знання життєвих позицій осіб, які скоюють злочинні діяння, їх ставлення до оточуючої дійсності, до людей, до суспільства. Це неможливо без вивчення їхніх потреб, інтересів, ціннісних орієнтацій, мотивів діяльності. Саме з'ясувавши стійкі, переважаючі в духовному житті індивіда інтереси до тих чи інших сфер соціального життя, явищ культури, ідеалів, можна отримати уявлення про спрямованість особи-злочинця [3, с. 78].

Світогляд, ціннісні орієнтації, інтелектуальні ознаки, емоційні особливості, вольові ознаки, культурний рівень, психічні аномалії, що не виключають осудність, рівень потреб та інші морально-психологічні ознаки особистості багатьох злочинців, досліджені науковцями значно менше, ніж інші ознаки, через труднощі, пов'язані передусім з методикою проведення таких досліджень [9, с. 110]. Це повною мірою стосується й такого специфічного (насамперед через особливості засобів вчинення злочинів) виду злочинності, як кіберзлочинність.

Як відомо, ціннісні орієнтації визначають ставлення людини до основних сфер життя, а також характеризують спрямованість особи загалом. Відповідно до цього критерію доречним є виокремлення таких типів злочинців:

1. *Соціально дезадаптований тип* – особи, характерними рисами яких є аутизація та інтравертність, тобто відхід у себе, відгородженість від навколишніх, спрямованість інтересів лише на задоволення своїх власних, в основному інформаційних потреб. Для злочинців даного типу інформативне спілкування й здійснення внаслідок цього кіберзлочину є засобом подолання дезадаптації. Для них досить важливим є прирахування себе до класу «хакерів», тобто ототожнення з однією з невеликих, але все-таки соціальних груп. Тим самим вони внутрішньо прагнуть подолати своє соціальне відчуження, відчути свою значимість, а також одержати можливість бути упевненим і зрозумілим у цьому соціальному середовищі. Щоб подолати власний психологічний дискомфорт, люди даного типу легко піддаються сторонньому негативному впливу, переймають «навколозлочинний» спосіб життя (24%).

2. *Емоційно сприйнятливий тип* – особи, які долучилися до вчинення кіберзлочинів для задоволення своїх особистих інтересів і потреб. Цей тип осіб має підвищену сприйнятливість і особливу чутливість до всього, що стосується інтересів особистості. В основному даний тип злочинців здійснює правопорушення з корисливих мотивів з метою задоволення своїх матеріальних потреб, рідше потреби в знаннях

та інших потреб. На відміну від правопорушників першого типу, це особи, що володіють лідерськими схильностями, з досить високим рівнем інтелекту. Вони самолюбні, проявляють завидну енергію й активність у досягненні поставлених цілей, гнучкість і легкість у спілкуванні, встановленні соціальних контактів. Однак досягнення своїх цілей «будь-яким шляхом» породжує в них почуття вищості й, відповідно, презирливе відношення до навколишніх, їм необхідний реальний успіх, щоб задовольнити свої потреби й честолюбство. Характерною для них є мінливість, відсутність прихильностей до кого-небудь, навіть до рідних й близьких, несприйняття й нерозуміння честі, гідності й обов'язку, нігілізм стосовно правових і моральних норм. Більшість кіберзлочинців належать саме до цього типу (48%).

3. *Соціально неадекватний тип* – представлений в основному молодими людьми з вищою освітою, високим інтелектуальним рівнем, матеріально забезпеченими. Корисливі мотиви й матеріальні потреби для них не відіграють ніякої ролі, на перший план виходить задоволення інших, нематеріальних потреб. Надмірні або незрозумілі з погляду навколишніх, але гадані природніми для особистості запити породжують проблему потреби промотиваційної сфери, яку неможливо дозволити через особисте небажання й неприйняття встановлених правових (соціальних) норм. Психологічний комфорт і зняття напруги досягаються цілеспрямованою діяльністю, що веде до бажаних результатів (28%) [10].

Таким чином, оскільки основна маса кіберзлочинців відноситься до другого типу, основним визначальним фактором деформації ціннісно-орієнтаційної сфери кіберзлочинця, тобто негативною рисою особистості, що найбільш сильно проявилася у кіберзлочинця при вчиненні кримінальних правопорушень, є корислива спрямованість особи.

Проведений нами аналіз матеріалів кримінальних проваджень показав, що характерними для кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, є наступні мотиви: користь (86%); помста (6%); потреба у самоствердженні та ігрові мотиви (3%); хуліганські мотиви (2%); кар'єризм (1%); інша особиста нематеріальна зацікавленість (2%).

Таким чином, слідчий на підставі аналізу слідів вчинення досліджуваної нами категорії кримінальних правопорушень може надати висновок про професіональний рівень користувача як злочинця, що зумовлений певною сукупністю ознак, як-от:

1) здатність злочинця використовувати технології анонімізації доступу до ресурсів мережі Інтернет (проксі-сервісів (комплексів програм), віртуальних приватних мереж, інших засобів-анонімайзерів). Вільний доступ користувачів до технологій анонімізації під час роботи в мережі Інтернет (проксі-сервісів (комплексів програм), віртуальних приватних мереж (VPN-технологій) та інших засобів-анонімайзерів) не означає, що кожний такий користувач використовує технологію правильно. Так, на форумах фахівці зазначають, що не можна закривати вкладку браузера з анонімайзером, а всі переходи здійснювати лише через неї (оскільки IP-адреса «фіксується» протягом усієї сесії в Інтернеті); жодним чином не можна використовувати легальні логін, пароль, поштову скриньку, реальні фотографії (відомості EXIF про фотографування), характерну для особи орфографію; необхідно враховувати специфіку дії анонімайзера (наприклад, Tor надає анонімність, а VPN приватність. Для банкінгу потрібна приватність, тому питання з приховуванням паролів відкрите, й вирішують його лише фахівці високої кваліфікації). І це лише окремі помилки, що мають наслідком викриття користувачів. Відчуття ж «невразливості» злочинця низького або середнього професіонального рівня може призвести й до більш вагомих помилок, які свідчать про ознаки злочинця;

2) мобільність злочинця (індивідуальна професійна, соціальна або географічна) [11, с. 38]. Мобільність означає здатність швидко орієнтуватися в ситуації, обирати найбільш доцільні форми діяльності [12, с. 682]. В інформаційному суспільстві комп'ютерні мережі та інші засоби інформаційно-комунікаційних технологій сприяють глобалізації, розвитку міжнародного ринку праці, вдосконаленню різних видів індивідуальної мобільності особи [11, с. 40]. Як види мобільності традиційно наводять географічну, соціальну та професійну. Географічну мобільність розглядають у контексті ринку праці: особа, діяльність якої забезпечує сфера телекомунікацій, може постійно змінювати

своє географічне місцезнаходження, працювати «дистанційно». Соціальну мобільність у соціології визначено як здатність людей у суспільстві переміщуватися між різними соціальними рівнями й економічними групами (економічна мобільність) [13, с. 840]. У кіберпросторі злочинець-користувач може бути суб'єктом багатьох соціальних спільнот (груп) у соціальних мережах, мати багато активних акаунтів (з англ. *account*) чи профілів, облікових записів, або ж узагалі не мати потреби в цьому. Варто додати, що географічна мобільність не завжди пов'язана з професійною, адже людина може мати високий ступінь географічної мобільності без можливості змінити особистий вибір і компетентність (роз'їзна робота з низьким рівнем професійної, соціальної та економічної мобільності) [11, с. 44];

3) психологічні характеристики (ознаки) злочинця, що впливають на формування й реалізацію злочинної мети. Злочинцям, що діють у кіберпросторі, притаманний вольовий компонент людської психіки. Воля – це свідоме управління людиною своєю діяльністю та поведінкою, що виявляється у прийнятті рішення, подоланні труднощів і перешкод на шляху досягнення мети, виконання поставлених задач;

4) роль у складі організованої злочинної групи [14, с. 114]. Криміналістичні аспекти щодо ролей учасників таких організованих груп перетинаються з кримінологічним дослідженням мережевої або корпоративної моделі як видів організованої групи, що протиставляються між собою [15, с. 81]. Корпоративній моделі притаманна централізована система, що має авторитарний характер; її схема є вертикаллю влади, елементи моделі можуть існувати паралельно з реальними структурами суспільства (державними або приватними). Для злочинних мереж, на відміну від корпоративних утворень, характерні непостійне членство й висока адаптивність до політичних, економічних і соціальних змін, що відбуваються в суспільному житті, без централізованої системи контролю. А. Л. Осипенко наводить визначальні чинники діяльності таких груп: 1) гнучке керування; 2) відносна рівноправність учасників групи, можливість змінення статусу (ролі) залежно від ситуації; 3) здатність до швидкого змінення складу групи та перерозподілу ролей; 4) швидкість відновлення втрачених злочинних зв'язків; 5) здатність виконувати те саме злочинне завдання застосуванням різного комплексу дій. Злочинець виконує певну роль у корпоративній або мережевій злочинній групі залежно від свого професіонального рівня.

Останнім часом спостерігається тенденція до збільшення кількості комп'ютерних злочинів кримінальними групами, що діють з метою викрадення грошових коштів найчастіше з банківських установ, або з іншою злочинною метою. Наприклад, для фізичного знищення важливого свідка, який знаходився в госпіталі під охороною. Після невдалих спроб його вбивства, злочинці, найнявши хакерів, через Інтернет проникли в локальну мережу цього госпіталю і змінили режим роботи кардіостимулятора та апарата штучної вентиляції легень, у результаті чого пацієнт помер. Його смерть, на перший погляд, здавалася цілком природною, лише після аналізу провайдером логічних файлів щодо доступу в локальну мережу, дійшли висновку, що несанкціоновано було змінено режим роботи кардіостимулятора [16, с. 29].

Кібертерористи. Терористичні організації все частіше використовують нові інформаційні технології та Інтернет із злочинним умислом щодо поповнення коштів, здійснення пропаганди або передачі секретної інформації. Такі терористичні угрупування, як Hizbollah, HAMAS, the AbuNidal organization, alQa'ida, використовують комп'ютерні файли, електронну пошту та шифрування (криптографію й комп'ютерну стеганографію) для підтримки своєї протиправної діяльності. Хоча терористи ще не застосовували кіберзброю за призначенням, проте вони використовують нові інформаційні технології й досягнення комп'ютерного прогресу, а це вже сигнал про небезпеку [16, с. 30].

Мережні шахраї. Використання Інтернет з метою шахрайства є, мабуть, сьогодні одним із найпоширеніших видів кіберзлочинів, з яким зіткнулися як приватні, так і державні структури всього світу. Тому, дуже важливо, щоб правоохоронні органи вивчили природу цих злочинів [16, с. 30].

Інтелектуальні піпрати. Інтелектуальна власність – це рушійна сила світового економічного прогресу в XXI столітті. Неліцен-

зійна продукція (піратство) загрожує економіці та суспільній безпеці, тому що вона здебільшого не відповідає стандартам якості. Зростання кількості низькоякісної піратської продукції зачепило й мережу Інтернет, де створено десятки тисяч вебсайтів виключно для поширення піратських матеріалів [16, с. 31].

Отже, можна стверджувати про доволі значний обсяг суб'єктів, які мають не тільки внутрішній, але й зовнішній доступ до комп'ютерної системи, що можуть розвивати протиправну діяльність завдяки системі спеціальних знань, умінь і навичок. Оперативний інтерес у ході виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, представляють такі особи: які не мають права доступу до певної інформації, що обробляється, не пов'язані трудовими відносинами з організацією чи фізичною особою – жертвою, але, можливо, мають деякі зв'язки з нею; співробітники організації, які мають право доступу до інформації, що обробляється у зв'язку із займаною посадою або спеціальними повноваженнями; співробітники організації (непосадові особи), які є користувачами та відносяться до персоналу, перебувають у трудових відносинах з власником технічних засобів (уповноваженою ним особою чи розпорядником) і визначені для здійснення функцій управління та обслуговування ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [17].

Таким чином, на підставі створеного узагальнюючого кримінологічного портрету злочинця, який вчиняє кримінальні правопорушення, пов'язані з обігом протиправного контенту в мережі Інтернет, зроблено висновок, що 89% випадків кримінальних правопорушень цієї групи вчиняються чоловіками віком близько 30–35 років, більше половини з яких неодружені, мають вищу або середню освіту, трохи менше половини з яких були офіційно працевлаштовані, хоча більше половини з них є працездатними, і на момент вчинення протиправних дій мали професію або навчалися. У 93% випадків особи, які вчинили такі кримінальні правопорушення, не мали кримінального минулого, майже 60% з них вчинювали їх самостійно і лише 11,8% – у складі організованої групи або злочинної організації. 100% злочинців були визнані судом осудними, 45% – засуджені. З'ясовано, що злочинці у кримінальних правопорушеннях, пов'язаних з обігом протиправного контенту в мережі Інтернету своїй більшості мислячі, творчі люди, у свідомості і поведінці яких, на жаль, переважають почуття помсти, заздрості і бажання довести своєму оточенню власне лідерство. Головною мотивацією їх вчинків є прагнення збагачення навіть під загрозою кримінального покарання.

ЛІТЕРАТУРА:

1. Хижняк Є. С. Процес встановлення особистості злочинців, які вчиняють злочини в мережі Інтернет. *Правові та інституційні механізми забезпечення розвитку України в умовах європейської інтеграції* : матеріали Міжнар. наук.-практ. конф. (Одеса, 18 трав. 2018 р.). Одеса: Видавничий дім «Гельветика», 2018. С. 424–427.

2. Тарасенко О. С. Теорія та практика протидії кримінальним правопорушенням, пов'язаних з обігом протиправного контенту в мережі Інтернет: *монографія*. Одеса : Видавничий дім «Гельветика», 2021. 432 с.

3. Борисова Л. В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права.* 2008. Вип. 44. С. 78.

4. Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: навч. посіб. / Українська академія внутрішніх справ. Київ, 1994. С. 15−16.

5. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: дис. ... канд. юрид. наук: 12.00.08 / НАН України; Інститут держави і права ім. В. М. Корецького. Київ, 2002. 198 с.

6. Джужа О. М., Василевич В. В., Чернєй В. В. та ін. Кримінологія : підручник / за заг. ред. В. В. Чернея, О. М. Джужі. Київ : ФОП Маслаков, 2020. 612 с.

7. Шеремет А. П. Злочини проти статевої свободи: монографія / Закарпат. держ. ун-т. Чернівці: Наші книги, 2008. 212 с.

8. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: дис. … канд. юрид. наук: 12.00.08. Харків, 2016. 213 с.

9. Антонян Ю. М. Социальная среда и формирование личности преступника (неблагоприятные влияния на личность в микросреде). Москва: Акад. МВД СССР, 1975. 159 с.

10. Криминологические и психологические характеристики личности преступника, совершающего преступления в сфере компьютерных технологий. URL: https://ozlib.com/980765/pravo/kriminologicheskie_psihologicheskie_harakteristiki_lichnosti_prestupnika_sovershayuschego_prestupleniya_sfer

11. Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність: системний підхід. *Інформаційні технології і засоби навчання.* 2015. № 5. Т. 49. С. 37–70.

12. Великий тлумачний словник сучасної української мови / гол. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. 1728 с.

13. Аніщенко В. М. Соціальна мобільність. *Енциклопедія освіти* / за ред. В. Г. Кременя. Київ : Юрінком Інтер, 2008. С. 840.

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

15. Корж В. П. Теоретические основы методики расследования преступлений, совершаемых организованными преступными образованиями в сфере экономической деятельности : монография. Харьков, 2002. 412 с.

16. Тарасенко О. С., Охріменко С. С., Стрільців О. М. Використання спеціальних знань під час розслідування несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку : *метод. реком.* К. : Нац. акад. внутр. справ, 2017. 74 с.

17. Тарасенко О. С. Вакуленко О. Ф., Стрільців О. М. та ін. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів : *метод. рек.* Київ, 2016. 55 с.