

## Форми вчинення транснаціональними злочинними організаціями окремих злочинів за допомогою використання мережі Інтернет



**Шепетько Сергій Анатолійович** – науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України

*Розглянуто причини поширення, надано коротку характеристику окремим злочинам, які вчиняються транснаціональними злочинними організаціями за допомогою мережі Інтернет, а також визначено заходи протидії таким злочинам.*

**Ключові слова:** кіберзлочинність, протидія, транснаціональна організована злочинність.

**Постановка проблеми.** Широке використання мережі Інтернет для оптимізації та автоматизації процесів у всіх без винятку сферах життєдіяльності призвело до нівелювання кордонів і глобалізації економіки та інформаційно-телекомунікаційної інфраструктури держав.

Зазначена тенденція має наслідком те, що кожен може отримати доступ до будь-якого виду відкритої інформації в будь-якій точці планети, навіть здійснювати дистанційно управління власними матеріальними благами та активами компанії без необхідності особистого контакту тощо.

Разом з цим, мережа Інтернет активно використовується транснаціональними злочинними організаціями як засіб вчинення злочину. Сьогодні підшукування або пристосування засобів знарядь, підшукування співучасників або змова на вчинення окремих злочинів не потребує безпосередньої присутності злочинця на території, де він буде вважатися закінченим. Новітні інформаційні технології дозволяють учасникам транснаціональної злочинної організації забезпечувати свою анонімність в умовах незначного ризику, а це надає їм можливість залучати

все більше людей до злочинної діяльності. Тому на сучасному етапі актуальним є питання протидії транснаціональній організованій злочинності, яка вчиняється з використанням мережі Інтернет.

**Стан дослідження.** У вітчизняній і зарубіжній юридичній літературі аналізу заходів протидії транснаціональній організованій злочинності завжди приділялася значна увага, оскільки такі злочини посягають на наявний порядок суспільних відносин, заподіюючи їм значної шкоди. В різні роки дослідженнями заходів протидії транснаціональній організованій злочинності, яка вчиняється за допомогою мережі Інтернет, займалися такі вчені, як В. М. Бутузов, М. Г. Вербенський, В. Д. Гавловський, В. О. Глушков, О. М. Джужа, Г. А. Зорін, Б. І. Калачов, Л. Л. Каневський, М. В. Корнієнко, Є. Д. Скулиш, В. Я. Тацій, О. М. Юрченко, В. А. Яценко та інші.

Праці зазначених учених мають вагоме значення для юридичної науки, у той же час складність виявлення та протидії проявам транснаціональної організованої злочинності, яка вчиняється за допомогою мережі Інтернет, унеможливає остаточне та однозначне вирішення цього питання. Саме це й обумовлює мету даної статті – визначити заходи протидії окремим проявам транснаціональної організованої злочинності, яка вчиняється за допомогою Інтернету.

**Виклад основного матеріалу.** Враховуючи незначну кількість зареєстрованих фактів транснаціональної організованої злочинності в Україні, важливо відмітити велику суспільну небезпечність кожного такого злочину, а також значний рівень латентності цієї злочинності, особливо завдяки використанню мережі Інтернет. Про незначну кількість випадків виявлення даного виду злочинності свідчать статистичні дані. Так, зокрема, за 3 місяці 2014 р. працівниками ОВС було виявлено 7 організованих груп і злочинних організацій з транснаціональними зв'язками, а за 3 місяці 2013 р. – 5 організованих груп і злочинних організацій з транснаціональними зв'язками. У порівнянні з минулим роком, цей показник збільшився на 40 %.

Відповідно до оцінок експертів, злочинність у мережі Інтернет здатна нанести збитки, які можливо порівняти з обсягом крадіжки виробів мистецтва в усьому світі. За даними ООН, збитки, які наносить така злочинність, можна порівняти з доходами від протизаконного обігу наркотиків і зброї. Крім того, дана злочинність виступає стримуючим фактором розвитку конкуренто-

спроможності економіки країн світу, в тому числі й України, оскільки покупці, підприємства та банки з пересторогою використовують нові технології – Інтернет-послуги [1, с. 338–339].

Така ситуація спричинена розширенням транснаціональними злочинними організаціями масштабів своєї діяльності завдяки використанню мережі Інтернет. Зокрема, на думку зарубіжних експертів, кількість неліцензійних сайтів у мережі Інтернет наразі більш ніж у десять разів перевищує ліцензійні. Значна кількість сайтів сьогодні працюють тільки в “Чорному Інтернеті”, а також використовують Інтернет як спосіб розрахунку віртуальною валютою чи електронними грошима. Як зазначає голова Європейського центру по боротьбі з кіберзлочинністю Трулс Ертінг: “Майже вся організована злочинність отримує прибуток у реальному світі за допомогою використання “віртуального світу”. Гроші, як правило, відмиваються в три етапи: розміщення (завантаження) – розшарування (класифікація, диференціація) та інтеграція. Гроші за допомогою мережі Інтернет постійно перебувають в обігу як усередині країни, так і між державами [2].

Злочинний дохід, отриманий транснаціональними злочинними організаціями від учинення окремих злочинів за допомогою мережі Інтернет, згодом може використовуватися для фінансування злочинних операцій, тероризму або насильницького екстремізму, сепаратизму. Завдяки мережі Інтернет відкриваються нові “бізнес-можливості” для отримання систематичних злочинних доходів в умовах незначного ризику.

Крім того, використати можливості мережі Інтернет для виявлення та притягнення винних осіб до кримінальної відповідальності можуть спеціальні підрозділи по боротьбі з організованою злочинністю. З цією метою доцільно створити спеціальні підрозділи у сфері фінансової розвідки, які будуть виявляти сайти, за допомогою яких здійснюється незаконний обіг електронних грошей. Оскільки завдяки використанню мережі Інтернет транснаціональні злочинні організації можуть отримувати значно більші злочинні доходи, необхідно терміново втілювати у практику діяльності вітчизняних правоохоронних органів, зокрема структурних підрозділів Головного управління по боротьбі з організованою злочинністю МВС України, активні заходи щодо співробітництва із зарубіжними правоохоронними органами з метою швидкого виявлення та припинення таких кримінальних правопорушень.

Зрозуміло, що без ефективної нормативно-правової та матеріально-технічної бази у сфері співробітництва правоохоронних органів різних іноземних держав неможливо ефективно протидіяти проявам транснаціональної організованої злочинності. Адже відсутність ефективних, скоординованих дій правоохоронних органів різних держав дозволяє учасникам транснаціональної злочинної організації уникати кримінальної відповідальності за вчинення окремих злочинів з використанням мережі Інтернет і постійно отримувати злочинні доходи. Наразі найменш ризикова-

ною та найбільш прибутковою діяльністю транснаціональних злочинних організацій з використанням мережі Інтернет є виготовлення, розповсюдження дитячої порнографії та піратство програмного забезпечення.

Зокрема, сьогодні дитяча порнографія проявляється в наступних аспектах: виготовлення, розподіл (розповсюдження) і завантаження фото та відеоматеріалу учасниками транснаціональної злочинної організації за допомогою мережі Інтернет, які знаходяться в різних країнах. Звісно, основним мотивом вчинення таких злочинів є отримання злочинного доходу.

Такий незаконний дохід отримують учасники транснаціональної злочинної організації шляхом надання будь-яким користувачам мережі Інтернет можливостей за власним бажанням користуватися (переглядати, завантажувати, обмінюватися даними) фото та відеоматеріалами, розміщеними на певному сайті. Такі прояви транснаціональної організованої злочинності за допомогою використання мережі Інтернет є одними із найбільш розповсюджених і, за оцінками експертів, приносять річний дохід у розмірі 3 млрд дол. США [3].

Сьогодні простежуються дві тенденції прояву дитячої порнографії: по-перше, все більшого поширення набувають такі форми вчинення злочину як створення незаконного матеріалу, а також збільшується кількість відео з дітьми, яких змушують виконувати статеві акти перед веб-камерою в режимі онлайн. Така форма вчинення злочину дозволяє користувачеві мережі Інтернет направляти онлайн запити на конкретні сексуальні дії, які він бажає щоб здійснювалися над жертвою в режимі реального часу. По-друге, на сайтах, де викладається дитяча порнографія, дотримуються заходів безпеки шляхом безпосереднього обміну файлами між користувачами, а не завантаження їх із сайту. Такі мережі є найбільш поширеними, тому часто використовуються для обміну файлами із фотографіями малолітніх дітей чи зображень сцен насильства над ними.

Дитяча порнографія та онлайн експлуатація дітей є транснаціональною організованою злочинністю. Філіппіни та Мексика займають провідні місця серед країн, де виробляють і поширюють дитячу порнографію, адже продукти цього злочину створюються і розповсюджуються по всьому світу. Тільки за березень 2014 р. було виявлено онлайн дитячу секс мережу, яка налічувала близько 250 дітей-жертв у 39 штатах США і п'яти країнах. Більшість із них – це хлопці віком від 13 до 15 років. Організація Об'єднаних Націй та Федеральне Бюро Розслідувань США виявили, що близько 750 000 “любителів дитячої порнографії” по всьому світу постійно підключені до мережі Інтернет у будь-який час доби [3].

Крім того, існує кілька проблем у боротьбі з онлайн дитячою експлуатацією. Першою проблемою є та, що мережа Інтернет – це сфера недостатнього нормативно-правового регулювання. Продовжують існувати законодавчі прогали-

ни у сфері правового регулювання діяльності Інтернет-провайдерів (ISP), проксі-серверів і платіжних сайтів. Наступна проблема пов'язана із недосконалістю механізму міжнародного співробітництва у сфері отримання інформації про транснаціональні злочинні організації, які діють за межами певної національної юрисдикції.

Дана проблема є наслідком того чинника, що багато країн мають недостатньо ефективне законодавство для протидії проявам дитячої порнографії. Зокрема, із 196 країн, де було проаналізовано національне законодавство, зарубіжними експертами зроблено висновок, що лише в 45 державах нормативно-правова база є достатньою для боротьби з поширенням дитячої порнографії, а у 89 із них узагалі відсутні правові норми у цій сфері [3].

Таким чином, у будь-якому гуманному суспільстві заходи щодо захисту дітей від онлайн-експлуатації учасниками транснаціональних злочинних організацій повинні бути невідкладними та пріоритетними. Щоб заходи боротьби з дитячою порнографією були ефективними, слід налагодити багатовекторне партнерство, яке б охоплювало національні та міжнародні правоохоронні органи, судові органи, Інтернет-провайдерів і підприємства, які надають інформаційно-телекомунікаційні послуги з метою запобігання, виявлення та припинення таких злочинів.

Переходячи до розгляду питання щодо піратства програмного забезпечення як проявів транснаціональної організованої злочинності, варто зауважити, що у квітні 2014 р. американський телевізійний канал "НВО" зламав піратські онлайн записи комп'ютерної гри "Тра престолів" з одного мільйона нелегальних сайтів на півдні США. Інтернет піратство в індустрії розваг коштує американській економіці більш ніж 12,5 млрд дол. США на рік. Майже чверть усього Інтернет-трафіку (за винятком порнографії), за оцінками експертів, порушує авторські права. Дослідження Альянсу Business Software показало, що 42 % комп'ютерного програмного забезпечення, яке використовується в усьому світі, є піратським, а в африканських країнах цей показник складає майже 80–90 %. Незаконний дохід від крадіжки програмного забезпечення становить 63,4 млрд дол. США [4].

Проведене Rand Corporation опитування громадян Бразилії показало, що 59 % респондентів не вважає скачування із таких сайтів порушенням авторських прав, а тим більше злочином. Таке ж опитування, проведене в Данії, також дозволяє зробити висновок, що 70 % респондентів вважають, що немає нічого незаконного в завантаженні піратського контенту із мережі Інтернет [4].

Крім того, дослідження Rand Corporation показало, що завдяки піратським сайтам злочинці заробляють навіть від такого легітимного доходу, як реклама, більш ніж 220 млн дол. США на рік. За оцінками експертів, організовані злочинні групи мають близько 4–5 млрд дол. США прибутку від продажу контрафактних компакт-дисків. Також Rand Corporation опублікувала доповідь щодо вивчення зв'язку між піратством,

організованою злочинністю та тероризмом. Так, у даній доповіді містилися переконливі матеріали щодо широкого, географічно розподіленого і постійного зв'язку між кінопіратством та організованою злочинністю, а також докази того, що терористичні групи, такі як Хезболла, використовували доходи від піратства фільмів для фінансування своєї діяльності [4].

Проведене пізніше в Бразилії дослідження дозволило також виявити зв'язки між злочинними організаціями, що незаконно збувають наркотичні засоби чи зброю, і тими, хто займається розважальним (ігровим) піратством. Бразильський випадок охарактеризував практику використання злочинними організаціями незаконних доходів від ігрового піратства як "План Б" для купівлі зброї і розширення територіального масштабу злочинної діяльності [4].

Таким чином, транснаціональні злочинні організації отримують величезні доходи від піратства та контрафакції товарів і це, по суті, є одним із самих високих їхніх злочинних доходів. Дослідження Rand Corporation показало, що маржа від піратства є набагато вищою, ніж від незаконного збуту наркотичних засобів та їх прекурсорів, і, що онлайн-операції у сфері піратства можуть повністю контролюватися за допомогою мережі Інтернет злочинними групами, що дозволяє їм постійно отримувати стабільний, незаконний дохід в умовах незначного ризику.

Крім вищезазначених злочинів, потенційними загрозами транснаціональної організованої злочинності з використанням мережі Інтернет можуть бути наступні протиправні діяння: 1) піратство програмного та ігрового забезпечення для мобільних телефонів, які активно використовуються споживачами для доступу до мережі Інтернет; 2) збут за допомогою мережі Інтернет програмного забезпечення, яке дозволяє друкувати зброю на 3D-принтері; 3) збут за допомогою мережі Інтернет аудіонаркотиків; 4) створення благодійних фондів, внески до яких можна перераховувати за допомогою мережі Інтернет шляхом переказу електронних грошей.

**Висновки.** Зважаючи на викладене, а також ураховуючи стрімкі процеси розвитку інформаційних технологій, особливо важливо, щоб оперативнорозшукові й кримінальні процесуальні заходи, які вживаються правоохоронними органами з метою протидії проявам транснаціональної організованої злочинності, були своєчасними та ефективними. При цьому, своєчасність та ефективність таких заходів залежить, насамперед, від наступних умов: 1) забезпечення надійного збереження інформаційної бази даних, яка використовується працівниками правоохоронних органів; 2) забезпечення збирання й вилучення доказів з електронного документообігу в осіб, які підозрюються в учиненні таких злочинів; 3) швидкого отримання оперативної інформації щодо фактів і обставин учинення злочину в мережі Інтернет; 4) встановлення місцезнаходження осіб, підозрюваних у учиненні злочинів за допомогою використання інформаційних

технологій; 5) забезпечення швидкого та ефективного обміну наявними оперативними даними, а також інформацією щодо проявів транснаціональної організованої злочинності між вітчизняними й іноземними правоохоронними органами.

Вдосконалення нормативно-правового забезпечення у сфері попередження та протидії проявам транснаціональної організованої злочинності з використанням мережі Інтернет можливе за умови: 1) внесення змін до КК України в частині посилення відповідальності за злочини у сфері комп'ютерних та інформаційних технологій, вчиненими учасниками транснаціональних злочинних організацій; 2) визнання електронних документів та інших даних у якості доказової бази при розслідуванні злочинів, учинених із використанням мережі Інтернет; 3) запровадження практики ідентифікації користувача мережі Інтернет шляхом надання оператором зв'язку при укладенні договору про надання інформаційно-комунікаційних послуг, ідентифікаційного коду особі.

#### **Список використаних джерел**

1. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби [Електронний ресурс] // Н. В. Савчук. – 2009. – С. 338–342. – Режим доступу : [http://tppe.econom.univ.kiev.ua/data/2009\\_19/zb19\\_48.pdf](http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf).

2. Cybercrime: getting paid and getting away with it / [Electronic resource]. – Mode of access :

<http://www.globalinitiative.net/cybercrime-getting-paid-and-getting-away-with-it/>.

3. Stolen innocence: the online exploitation of children / [Electronic resource]. – Mode of access :

<http://www.globalinitiative.net/stolen-innocence-the-online-exploitation-of-children/>.

4. Entertainment piracy: fair game, or organized crime? / [Electronic resource]. – Mode of access :

<http://www.globalinitiative.net/online-piracy/>.

*Рассмотрены причины распространения, надана краткая характеристика отдельных преступлений, совершаемых транснациональными преступными организациями с помощью сети Интернет, а также определены меры противодействия таким преступлениям.*

*The article considers the causes of distribution, and provided a brief description of certain crimes committed by the transnational criminal organizations through the Internet, and determined the measures to combat these crimes.*

*Стаття надійшла до редакції журналу 22 квітня 2014 року.*