

УДК 343.575

ПРОТИДІЯ НАРКОЗЛОЧИННОСТІ В МЕРЕЖІ ІНТЕРНЕТ: ВИКЛИКИ СЬОГОДЕННЯ

COUNTERACTION TO DRUG CRIME IN THE INTERNET: CURRENT CHALLENGES

Ступник Я.В.,

*кандидат юридичних наук,
доцент кафедри кримінально-правових дисциплін
та міжнародного кримінального права
ДВНЗ «Ужгородський національний університет»*

Когут М.Г.,

*юридичний факультет
ДВНЗ «Ужгородський національний університет»*

У статті досліджуються проблемні питання запобігання та протидії наркозлочинності у всесвітній комп'ютерній мережі Інтернет, а також проводиться аналіз практики кримінологічного впливу на наркозлочинність у сфері сучасних інформаційних технологій.

Ключові слова: наркозлочинність, наркобізнес, наркотичні засоби, кіберзлочинність, Інтернет.

В статье исследуются проблемные вопросы предотвращения и противодействия наркопреступности во всемирной компьютерной сети Интернет, а также проводится анализ практики криминологического воздействия на наркопреступность в сфере современных информационных технологий.

Ключевые слова: наркопреступность, наркобизнес, наркотические средства, киберпреступность, Интернет.

Scientific article is devoted to the range of problems of distribution of the virtual drug dealing in the network of Internet, to description of him basic displays, analysis of international experience in this question, and development of methods of fight against them. Drug crimes present a considerable danger for society, pulling after itself not only a threat to life and physical health of man but also to psychological firmness of whole society

Key words: drug criminality, drug dealing, drug facility, cybercrime, Internet.

Постановка проблеми. Наші знання про сучасні комп'ютерні технології, апаратні і програмні засоби, а також їх сучасні можливості, за великим рахунком, залишаються фрагментарними. І це при тому, що

розглядувана проблематика вже більше 20 років повертає до себе пильну увагу вчених і практиків, які цікавляться питаннями протидії злочинності. З усією очевидністю можна стверджувати, що поставле-

них і невирішених питань тут набагато більше, ніж запропонованих відповідей.

З іншого боку, можна спостерігати деяку демонізацію комп'ютерної злочинності, обумовлену, в першу чергу, нерозумінням природи і суті процесів, що відбуваються у відповідному середовищі. Дійсно, тут не працюють багато традиційних правоохоронних та профілактичних заходів та процедур, а можливості соціального контролю – досить обмежені [1, с. 3].

Окремі аспекти розглянутих питань були предметом досліджень ряду вітчизняних та закордонних вчених, зокрема таких, як Т. Виноградська, В. Голубєв, А. Гуров, В. Зимовець, Б. Калачов, В. Кузьмінов, О. Литвак, А. Рокітов, М. Салтевський, І. Смирнова, А. Рокитов, Д. Чувірін та ін.

Метою цієї публікації є доктринальний аналіз окремих проблем протидії наркозлочинності в мережі Інтернет та вироблення пропозицій щодо їх вирішення на рівні законодавства про кримінальну відповідальність.

Виклад основного матеріалу. На початку нового тисячоліття в результаті науково-технічного прогресу суспільство реально відчуває наступ інформаційної революції. Її сутність вчені зводять до зміни технічних основ способів передачі, зберігання і обробки інформації, розвитку проводового і радіозв'язку, появі телебачення, що дозволяє більшій кількості людей бути причетними до світу подій. «Інформаційна революція змінює суспільну свідомість всього людства, – зазначає К.К. Колін, – робить його більш глобальним».

Україна, будучи органічною частиною світової спільноти, не може бути в цьому зв'язку винятком. Становлення ринкової економіки, поява нових її галузей, лібералізація сфери інформаційних суспільних відносин сприяли справжньому розквіту комп'ютерної злочинності.

Що стосується проблеми кваліфікації злочинних дій з наркотичними засобами і психотропними речовинами, то організація дієвої протидії цим організованим злочинам в україномовному сегменті мережі Інтернет є для діяльності правоохоронних органів України новою і тому представляє значний інтерес як для вітчизняних практичних працівників, так і для науковців.

Прогалина у даній сфері наукового знання негативно позначається на організації міжвідомчої протидії і профілактики віртуального наркобізнесу, на законотворчій практиці, яка мала б регламентувати ці суспільні відносини. До недоліків наукового, законодавчого, правозастосовного рівня додається ще і брак відповідних методик розкриття і розслідування даного виду злочинів, фахівців і високотехнологічного програмно-пошукового забезпечення в Мережі, висока латентність Інтернет-наркобізнесу і т. ін.

Тому актуальність вивчення використання мережі Інтернет наркобізнесом для реалізації безконтактних оборотів пов'язана з необхідністю вироблення дієвої системи профілактики і протидії злочинній діяльності в електронних ресурсах мережі Інтернет,

а також – із намаганнями заповнити вакуум у розглядуваній сфері.

Злочинна діяльність у сфері незаконного наркобізнесу є складною, структурованою, відрізняється вчиненням наркотичних злочинів з кваліфікуючими та особливо кваліфікуючими ознаками, що проявляє себе у діяльності груп осіб за попередньою змовою, організованих груп і злочинних організацій стосовно наркозасобів у великих і особливо великих розмірах з міжнародними і транснаціональними зв'язками. Ділки наркокриміналітету вже давно оцінили досягнення науково-технічного прогресу в сфері новітніх технологій, де завдяки своєму глобальному характеру і швидким темпам розвитку саме Інтернет став їх квінтесенцією [2, с. 1].

У зв'язку з розвитком сучасних комп'ютерних технологій, насамперед всесвітньої електронної мережі Інтернет, в міжнародному законодавстві з'явився новий термін «кіберзлочинність» [3].

Комп'ютерні (мережеві) злочини можна поділити на дві групи:

1. Злочини, що безпосередньо посягають на безпеку комп'ютерних систем та комп'ютерної інформації;

2. Злочини проти особистості, власності, порядку управління та інших об'єктів, але які вчиняються з використанням комп'ютерів, комп'ютерних систем і сучасних мережевих технологій.

Останній тип незаконних дій, власне, і належить до кіберзлочинності. Кіберзлочинність в силу своєї специфіки стала настільки актуальним явищем, що в листопаді 2001 року Радою Європи була прийнята Конвенція про кіберзлочинність (Ратифікація від 07.09.2005).

Слід відмітити, що фірми Microsoft, AT & T, Apple відмовилися від приватних електронних мереж на користь мережі Інтернет, яка жадібно поглинає приватні інформаційні мережі, перетворюючи Інтернет в світову павутину. Глобалізація мережі Інтернет має очевидну тенденцію до подальшого розширення, стає звичним атрибутом сучасного життя.

Важко переоцінити можливості, які відкриває це вікно у світ для розвитку творчих здібностей особистості, бізнесу, науки. Музеї та бібліотеки світу відкривають перед вашим поглядом свої скарби, банки відкривають рахунки, товари переміщуються по всьому світу як за помахом чарівної палички.

Експерт ООН, координатор Програми ООН з контролю над наркотиками Сандіп Шоула зробив заяву, що Інтернет став таємною лабораторією для виготовлення синтетичних наркотиків. Згідно з наведеними ним даними мережа Інтернет виявилася засмічена рецептами виробництва і споживання наркотиків, головним чином синтетичних препаратів нових поколінь.

У порівнянні з іншими державами таке використання Інтернету в нашій країні ще тільки розгортається, але репрезентативний аналіз веб-сторінок, відведених під рубрику «наркотики», показує, що понад 80 відсотків відводиться інформації, м'яко кажучи, негативної. При цьому переважна частка

інформації – 77,8 відсотка – стосується так званих важких наркотиків типу амфетамінів, галюциногенів і інших. Цей показник для україномовного Інтернету в 1,5 рази вище, ніж для Інтернету в глобальних масштабах. А «важкі» наркотики – одні з найнебезпечніших, і звикають до них швидше, і наслідки їх вживання є значно важчими.

Сьогодні Інтернет, з його практично необмеженими інформаційно-комунікативними можливостями, використовується наркоугрупованнями в якості інструмента просування на ринок свого забороненого товару. З цією метою в Мережі активно рекламуються психоактивні речовини і наркотична субкультура, психоделічна філософія. На багатьох сайтах пронаркотичного спрямування знаходиться чимало текстів з описом різних видів наркотичних засобів і психотропних речовин та рецептів їх вироблення, виготовлення, виробництва та споживання. Даються поради, як поводити себе при затриманні працівниками правоохоронних органів за зберігання і перевезення наркотиків [4, с. 141-149].

Сучасні комп'ютерні технології сприяли інтеграції економіки в єдину глобальну систему, стан якої в значній мірі визначається функціонуванням фондових бірж та ринків капіталу. Однак технічний прогрес і глобалізація в сфері торгівлі та фінансової діяльності відкрили можливості не тільки для соціального розвитку, але й для появи нових і розвитку традиційних форм злочинності. У зв'язку з цим і з'явився термін «кіберзлочинність». Він охоплює різні види діяльності і використовується для позначення будь-яких порушень закону, при здійсненні яких або сприяння вчиненню яких використовуються електронні засоби [5, с. 45].

Особливості кіберзлочинів полягають у наступному:

1. При використанні невеликих ресурсів для їх здійснення може бути завдано величезної шкоди;
2. Злочин може бути вчинений в межах однієї юрисдикції (країни), а правопорушник може перебувати під іншою юрисдикцією (в іншій країні);
3. У багатьох національних законодавствах відсутнє чітке визначення (чи якесь визначення взагалі) таких правопорушень;
4. Небезпека, що загрожує правопорушникам, і ймовірність їх виявлення досить низькі.

Найбільш значущим на сьогоднішній день результатом міжнародного співробітництва в боротьбі зі злочинністю, пов'язаною з використанням високотехнологій, є Конвенція Ради Європи про кіберзлочинність [6]. У підготовці тексту брали участь 43 держави – члени Ради, а також Канада, Японія, Сполучені Штати (які мають статус спостерігачів) і Південно-Африканська Республіка. Конвенція була прийнята 8 листопада 2001 року і відкрита для підписання 23 листопада 2001 року.

У Конвенції зачіпаються питання юрисдикції, видачі, перехоплення повідомлень, а також формування та збереження даних. У ній перераховуються діяння, які мають бути визнані кримінально караними відповідно до національного законодавства, в тому

числі: несанкціонований доступ, незаконне перехоплення даних, порушення цілісності даних, порушення цілісності систем, пов'язане з використанням комп'ютерів підроблення, пов'язане з використанням комп'ютерів шахрайство, пособництво чи підбурювання до вчинення цих злочинів.

У Конвенції докладно розглядається механізм налагодження ефективного міжнародного співробітництва та координації при проведенні розслідувань і кримінального переслідування. Зокрема, сторони цієї конвенції повинні наділити національні органи повноваженнями здійснювати комп'ютерний пошук і вилучати комп'ютерні дані.

В рамках розслідування справ, пов'язаних з наркотиками, конвенція застосовується в якості засобу забезпечення взаємної юридичної допомоги. Наприклад, компетентні органи, які прагнуть отримати електронні докази діяльності торговців наркотиками і виявити їх клієнтів або їх активи в іншій державі, можуть звертатися до такої держави з проханням про пошук баз даних, які використовувалися підозрюваними в занятті наркобізнесом особами, або про перехоплення їх електронних повідомлень, наприклад електронної пошти [1, с. 63-64].

Однак представники приватного бізнесу і громадські об'єднання виступають проти деяких положень конвенції про кіберзлочинність. Консорціум асоціацій, що об'єднують підприємства з виробництва інформаційних технологій, заявив про свої заперечення в зв'язку з тим, що конвенція, на його думку, покладає на постачальників послуг у мережі Інтернет обтяжливі обов'язки по зберіганню даних і відповідальність за дії третіх сторін, а також обмежує масштаби законної діяльності в Інтернеті. Групи боротьби за громадянські свободи зробили аналогічні заяви про свою стурбованість передбаченими в конвенції заходами, які, на їхню думку, являють собою посягання на недоторканність приватного життя. Міжнародний комітет ООН з контролю над наркотиками (МККН) вважає, що такий правовий документ сприяє здійсненню зусиль по боротьбі з незаконним обігом наркотиків та зловживанням ними.

До способів незаконного використання сучасних технологій наркототорговцями МККН відносить наступні [7]:

- поширення за допомогою засобів масової інформації, в тому числі електронних, інформаційних матеріалів, що підбурюють чи спонукають до вживання наркотиків (порушення статті 3 Конвенції ООН про боротьбу проти незаконного обігу наркотичних засобів і психотропних речовин 1988 року);
- поширення через мережу Інтернет інформації, що містить рекомендації щодо незаконного використання та виготовлення наркотиків.

Формули (прописи) наркотиків зазвичай трималися в секреті, вони ревно охоронялися, а при сучасних засобах інформатизації відомості про них може тепер отримати кожен, хто здатний вийти на оператора, підключеного до глобальної мережі. Тепер навіть малокваліфіковані фахівці мають електронний шлях залучення до виробництва наркотиків. Менше 10

відсотків підозрілих осіб, затриманих за незаконне виробництво метамфетаміну, є експериментальними хіміками, що і пояснює причину численних спалахів, вибухів і нещасних випадків з пораненнями, які відбуваються в підпільних лабораторіях.

Крім того, в мережі Інтернет відбувається нерегламентоване зростання числа аптек, які пропонують до продажу препарати, в тому числі сильнодіючі та нарковмісні, без жодного рецепта (що є порушенням статті 10 Конвенції ООН про психотропні речовини 1971 року).

Новітні технології дозволяють групам наркобізнесу застосовувати наступні методи при скоєнні злочинів.

1. Приховування електронної інформації про постачання незаконних партій наркотиків:

А. Шляхом кодування електронних послань.

Б. Шляхом використання неконтрольованих засобів електронного зв'язку.

2. Відмивання доходів від наркобізнесу за допомогою електронних переказів:

Інтернет володіє трьома специфічними властивостями, які можуть сприяти відмиванню грошей вільним доступом, анонімністю відносин між клієнтом та фінансовою установою, високою швидкістю здійснення електронних угод [8, с. 135].

Поява нових світових ринків акцій, облігацій, ф'ючерсів, валюти та інших цінних паперів розширює коло операцій, що здійснюються за допомогою електронних засобів швидко, легко і скритно переміщати по світу великі суми грошей. Використання смарт-карт і он-лайнних механізмів здійснення банківських операцій обмежує особисті контакти між співробітниками банків і клієнтами, а значить, знижує дієвість механізмів перевірки законності фінансової діяльності. Конкуренція в сфері фінансових послуг сприяє тому, що найчастіше заходи боротьби з відмиванням грошей розглядаються як несумісні з нормальною діловою практикою [9].

Спеціальні комп'ютерні програми судової експертизи дозволяють застосовувати комп'ютерні техніку і технології для обробки інформації про вилучені докази і отримувати з комп'ютерних систем необхідну інформацію для слідчих або оперативних цілей. Комп'ютерні програми можуть відслідковувати масиви даних за ключовими словами або словосполученнями або виявляти окремі елементи електронних повідомлень, які відповідають заданим параметрам фільтра, встановленого у відповідності з рішенням суду, наприклад, повідомлення, адресовані певному рахунку, або користувачеві або виходять від такого рахунку або користувача. При оновленні програм функції контролю цілісності фіксують режим збору даних, який використовувався щодо доказів, і показують, що застосовувалися параметри фільтра і отримана інформація не змінилася. Такі функції є додатковим підтвердженням автентичності та недоторканності ланцюга процедур забезпечення збереження даних [10, с. 45].

Спеціальні комп'ютерні моделі для виявлення в он-лайнному режимі відхилень у фінансових опе-

раціях і розробка програмного забезпечення для високошвидкісних комп'ютерів дозволяють встановлювати особу торговців наркотиками за відбитками пальців. З їх допомогою створюються інформаційні мережі, що дають можливість компетентним органам робити перехресні посилання між даними реєстрації прав власності та іншими даними, до прикладу, податковими деклараціями.

В даний час митні органи та органи, що займаються інспекцією вантажів, володіють різними засобами догляду, які дозволяють проводити огляд без застосування заходів примусу. Для цього використовуються вдосконалені методи виявлення за допомогою рентгенівського і гамма-випромінювання. Також створюються переносні (пересувні) пристрої для пошуку наркотиків на судах, в каютах і контейнерах будь-яких розмірів в процесі огляду на морі та в портах. Цілковито виправдовують себе методи швидкого огляду пасажирів та їх багажу, які дозволяють не створювати зайвих незручностей для громадян.

Співпраця правоохоронних органів і спецслужб з приватним сектором економіки є основою організації більш ефективного відсічі злочинності, пов'язаної з використанням високих технологій, і захисту від неї. Постачальники послуг в Інтернеті створюють міжнародні мережі співпраці з правоохоронними органами на основі так званих асоціацій ліній екстреного зв'язку. Ці мережі в основному взаємодіють з метою боротьби з дитячою порнографією в мережі Інтернет. У разі виявлення матеріалу, який кваліфікується як дитяча порнографія, лінія екстреного зв'язку встановлює місцезнаходження сайту і, якщо він розташований в безпосередній близькості, повідомляє про це поліцію і (або) постачальника послуг в Інтернеті. Потім виявлений матеріал усувається за допомогою чітко сформульованого повідомлення та процедур ліквідації. Багато країн застосовують аналогічні національні системи. За такою схемою можна вибудовувати взаємодію з приватним сектором економіки для припинення поширення незаконної інформації про наркотики в Інтернеті [11, с. 3].

Висновки. Підводячи підсумки, є підстави сформулювати наступні пропозиції щодо подальшого вдосконалення регламентації кримінологічних засобів впливу на наркозлочинність в мережі Інтернет. По-перше, потребується термінове обговорення і прийняття Закону України «Про перехоплення телекомунікацій», яким передбачити законодавчі засади попередження і припинення злочинних дій, у тому числі з наркотичними речовинами в мережі Інтернет. По-друге, необхідним є створення Національного (міжвідомчого) управління оперативного/мобільного реагування на базі СБ України і Департаменту по боротьбі з незаконним обігом наркотиків МВС України з функціями моніторингу і відстеження використання наркобізнесом мережі Інтернет із застосуванням антинаркотичної СОРЗ. По-третє, слід передбачити нормативно-правове залучення до процесу дослідження змістовної спрямованості та прихованого, кодованого, жаргонізованого мовлення сайтів мобільної групи з числа відповідних

спеціалістів: лінгвістів і нейролінгвістів, психологів, експертів-криміналістів і кримінологів. По-четверте, кожен громадянин самостійно за короткий термін може легко відшукати сайт в українському сегменті Інтернет, що пропонує безпечно придбання наркоспособу. Таким чином, кожен користувач мережі, у тому числі й неповнолітній, може купувати заборонені наркотики, тому необхідно розробити систему заохочення за конфіденційне повідомлення через «гарячу» телефонну лінію на кшталт американського досвіду про подібні повідомлення громадян через оперативний канал «Біла скринька» про торгівлю наркотиками в Інтернет до правоохоронних органів України. По-п'яте, в Україні необхідна розробка і запровадження спеціального програмного забезпечення щодо моніторингу та інтелектуального блоку-

вання (відключення) сайтів пронаркотичного спрямування. Як приклад, у США для подібних цілей виділяється близько 35 млрд. дол., у Росії до 2015 року планується обладнати всі шкільні комп'ютери антинаркотичними фільтрами Інтернет-ресурсів вартістю приблизно 50 млн. дол. США. По-шосте, необхідними є розробка та імперативне (обов'язкове) для провайдерів розташування в україномовному сегменті Інтернет на молодіжних сторінках антинаркотичної реклами на зразок яскравих баннерів з візуальними зображеннями.

Слід пам'ятати, що наркотики – це одне із найнебезпечніших явищ в нашому суспільстві. Вони сприяють лише його деградації та занепаду. Власне кажучи, мова йде про загрозу генофонду нації і національній безпеці України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Семерак О.С., Ступник Я.В., Сливич І.І. Наркозлочинність: кримінологічна та кримінально-правова характеристика: Науково-практичний посібник. – Ужгород. : Бреза, 2013.
2. Кузнецов С. Профілактика наркоманії та наркозлочинності в молодіжному середовищі [Електронний ресурс] / С. Кузнецов. – Режим доступу : <http://i-gazeta.com/narkostop/23127.html>.
3. Зимовець В.В., Смирнова І.В., Чувирін Д.Е. Запобігання віртуальному наркобізнесу в Internet: перспективи для України / В.В. Зимовець, І.В. Смирнова, Д.Е. Чувирін // Науково-практичний журнал «Боротьба з організованою злочинністю і корупцією (теорія і практика)». – № 16 – 2007 (http://mndc.naiu.kiev.ua/Gurnal/16text/g16_05.htm).
4. Литвак О. Латентна злочинність: деякі аспекти / О. Литвак // Право України. – 2003. – № 1.
5. Волощук А.М. Державно-правова політика в сфері протидії незаконному обігу наркотичних засобів, психотропних речовин та прекурсорів: зарубіжний досвід / А.М. Волощук // Митна справа (Митний комплект). – 2011. – № 1.
6. Конвенція про кіберзлочинність. Рада Європи; Міжнародний документ від 23.11.2001. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_575.
7. Golubev V. Creating conditions for constructive international coopération in combating the transnational computer crime — is the demand of the time // The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, to be held in Vienna, Austria, from 15 April 2000.
8. Смирнова І.В. Організована злочинна діяльність у сфері незаконного обігу наркотичних засобів: загальне поняття стадій / І.В. Смирнова // Наук. вісник Нац. акад. внутр. справ України: НАВСУ, 2005. – № 1.
9. Волощук А.М. Державно-правова політика в сфері протидії незаконному обігу наркотичних засобів, психотропних речовин та прекурсорів: зарубіжний досвід / А.М. Волощук // Митна справа (Митний комплект). – 2011. – № 1.
10. Рокитов А.І. Філософія комп'ютерної революції. – М., 1991.
11. Салтевський М.В., Литвинов О.М., Чернец Н.Г. Проблеми протидії злочинності в сфері комп'ютерних технологій: Науково-практичний посібник. – М. : Юркнига, 2006.