УДК 343.9.024:004.056.5
DOI https://doi.org/10.32850/sulj.2022.3.29

ВЗАЄМОЗВ'ЯЗКИ МІЖ ОКРЕМИМИ ФОРМАМИ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ У СФЕРІ ЕКОНОМІКИ ТА ФУНКЦІОНУВАННЯМ КІБЕРПРОСТОРУ

Куліуш В.М.

Метою статті є виокремлення та характеристика основних форм взаємозв'язків між злочинною діяльністю у сфері економіки та функціонуванням кіберпростору. Акцентована увага на швидкому та динамічному розвитку засобів цифрового зв'язку та комунікацій, що призвело до розвитку цифрової економіки, а також появи нових форм загроз функціонуванню економічної системи, побудованої на цифрових платформах. Виокремлено основні та системні ознаки цифрової економіки, а також охарактеризовано основні її елементи. Наголошено на швидкій адаптивності злочинності, яка інтенсивно освоює нові ніші та соціальні практики. На підставі аналізу наявних наукових підходів виокремлено основні форми взаємозв'язків між розвитком та функціонуванням кіберпростору та окремими формами злочинної діяльності у сфері економіки. Звернута увага на системному характері таких взаємозв'язків.

Детально охарактеризовано вплив кіберпростору на криміналізацію окремих форм діянь у сфері економіки. Охарактеризовано концептуальний підхід у галузі кримінального права щодо вирішення цієї проблеми. Проаналізовано вплив кіберпростору на якісну трансформацію інфраструктури економічної злочинності. Виокремлено та охарактеризовано основні функції кіберпростору як інфраструктурного елемента економічної злочинності. Детально проаналізовано сегменти мережі Інтернет, які не індексуються традиційними пошуковими системами та звернута увага на появу нового феномену – цифрових кримінальних ринків. Вперше запропоновано визначення цифрового кримінального ринку, під яким розуміється стійка, централізовано не контрольована система, яка здатна до самовідтворення і саморегуляції, спрямована на створення з урахуванням структури та динаміки попиту пропозиції заборонених у цивільному обігу товарів та послуг у кіберпросторі.

Визначено основні ознаки цифрових кримінальних ринків, а також охарактеризовано найбільш розвинуті їх сегменти.

Ключові слова: *злочинна діяльність у сфері економіки, кіберпростір, високі інформаційні технології, взаємозв'язки, інфраструктура злочинності, цифрові кримінальні ринки.*

Kuliush V. M. Interrelationships between separate forms of criminal activity in the economic sphere and the functioning of cyberspace

The purpose of the article is to highlight and characterize the main forms of relationships between criminal activity in the economic sphere and the functioning of cyberspace. Attention is focused on the rapid and dynamic development of digital means of communication and communications, which has led to the development of the digital economy, as well as the emergence of new forms of threats to the functioning of the economic system built on digital platforms. The main and systemic features of the digital economy are singled out, as well as its main elements are characterized. The rapid adaptability of crime, which is intensively mastering new niches and social practices, is emphasized. Based on the analysis of available scientific approaches, the main forms of interrelationships between the development and functioning of cyberspace and individual forms of criminal activity in the economic sphere are singled out. Attention is drawn to the systemic nature of such relationships.

The impact of cyberspace on the criminalization of certain forms of actions in the economic sphere is described in detail. The conceptual approach in the field of criminal law to solving this problem is characterized. The influence of cyberspace on the qualitative transformation of the infrastructure of economic crime is analysed. The main functions of cyberspace as an infrastructural element of economic crime are singled out and characterized. Segments of the Internet that are not indexed by traditional search engines are analysed in detail, and attention is paid to the emergence of a new phenomenon – digital criminal markets. For the first time, the definition of the digital criminal market is proposed, which means a stable, not centrally controlled system that is capable of self-reproduction and self-regulation, aimed at creating, taking into account the structure and dynamics of demand, the supply of goods and services prohibited in civil circulation in cyberspace.

The main features of digital criminal markets are defined, and their most developed segments are also characterized.

Key words: *criminal activity in the economic sphere, cyberspace, high information technologies, interconnections, crime infrastructure, digital criminal markets.*

Постановка проблеми та її актуальність. Як відзначають вчені-економісти, основним глобальним трендом сучасного суспільного буття є все більш прогресуючий перехід у віртуальний інформаційний простір – онлайн. Цій об'єктивній революційній зміні неможливо і безглуздо чинити опір. Але можливо і вкрай необхідно враховувати нові тенденції і нові загрози. Революція у сфері зв'язку та комунікацій стала суттєвим чинником розвитку цифрової економіки, світового економічного зростання та вагомим інструментом забезпечення сталого розвитку. З одного боку, це дало можливість підприємствам та споживачам в усьому світі отримати вигоди від ефективності, швидкості та зручності цифрових операцій та обміну інформацією, а з іншого – зумовило зростання ймовірності отримання фінансових збитків, витоку даних та репутаційних збитків через кіберзлочинні дії [3].

Аналітики слушно відзначають, що цифрова економіка істотно змінює традиційні бізнес-процеси. За досягнення найбільш складних рівнів цифровізації в економіці відбувається кардинальна трансформація виробничих відносин учасників, результатом якої є об'єднання виробництва і послуг в єдину (цифрову) систему, у якій: *по-перше*, усі елементи економічної системи присутні одночасно у вигляді фізичних об'єктів, продуктів і процесів, а також їх цифрових копій (математичних моделей); *по-друге*, усі фізичні об'єкти, продукти і процеси за рахунок наявності цифрової копії та елемента «підключеності» стають частиною інтегрованої IT-системи; *по-третє*, через наявність цифрових копій (математичних моделей) і будучи частиною єдиної системи, всі елементи економічної системи безперервно взаємодіють між собою в режимі близькому до реального часу, моделюють реальні процеси і прогнозовані етапи, забезпечують постійну оптимізацію усієї системи. Продовжуючи, аналітики звертають увагу, що основними сегментами цифрової економіки є: а) сектор інформаційно-телекомунікаційних технологій, інфраструктура електронного бізнесу (мережі, софтвер, комп'ютери тощо); б) цифрове виробництво та електронний бізнес, тобто процеси організації бізнесу із використанням комп'ютерних мереж; в) електронна торгівля, тобто роздрібні Інтернет-продажі товарів [5].

Наведені процеси не залишилися поза увагою злочинності, яка характеризується адаптивністю та відносно швидко підлаштовує протиправні соціальні практики до нових реалій, а іноді й використовує їх для формування нових сегментів злочинної діяльності та кримінальних ринків, що і зумовлює необхідність вивчення системи взаємозв'язків між розвитком кіберпростору та окремими формами злочинної діяльності економічної спрямованості.

Аналіз останніх досліджень та публікацій. Останніми роками питання виявлення та розслідування злочинів, які вчиняються із використанням кіберпростору, зокрема й злочинів економічної спрямованості досліджувалось значною кількістю науковців, зокрема: П.Д. Біленчуком, А.С. Білоусовим, І.О. Вороновим, В.Д. Гавловським, М.В. Карчевським, О.М. Лепехою, М.Ю. Літвіновим, О.І. Мотляхом, Л.П. Паламарчук, Д.В. Пашнєвим, Б.В. Романюком, О.А. Самойленко, К.В. Тітуніною, Д. М. Цеханом та іншими науковцями.

Метою статті є визначення основних взаємозв'язків між розвитком кіберпростору та злочинною діяльністю у сфері економіки.

Виклад основного матеріалу. Переходячи до безпосереднього аналізу взаємозв'язків між розвитком кіберпростору та окремими формами злочинної діяльності, слушно звернути увагу на позицію Д.М. Цехана, який відзначає, що взаємозв'язки високих інформаційних технологій зі злочинною діяльністю проявляються у трьох напрямах: *по-перше,* поява інноваційних форм злочинної діяльності; *по-друге,* модифікація «традиційних» механізмів вчинення злочинів, а саме способу та особи злочинця; *по-третє*, створення інноваційних техніко-соціальних середовищ, що з часом криміналізуються та використовуються в окремих формах злочинної діяльності [4]. Загалом така позиція підтримується нами щодо взаємозв'язків високих інформаційних технологій та злочинності загалом. Водночас аналітичний огляд наукових робіт, вивчення матеріалів оперативно-розшукових справ, кримінальних проваджень та проведене опитування працівників правоохоронних органів свідчить, що у контексті економічної злочинності наведена система взаємозв'язків має дещо інший характер, який потребує додаткового дослідження.

Так, сьогодні можна констатувати, що взаємозв'язки між розвитком кіберпростору та окремими формами злочинної діяльності у сфері еко-

номіки проявляються у таким формах: *по-перше*, криміналізація окремих діянь, зумовлена широкомасштабним впровадженням високих інформаційних технологій та їх структурної складової частини – кіберпростору у всі форми суспільного життя; *по-друге*, якісна трансформація інфраструктури економічної злочинності, що зумовлено перетворенням кіберпростору у невід'ємну складову частину економічних відносин; *по-третє*, трансформація окремих способів вчинення економічних злочинів у складні технології злочинної діяльності; *по-четверте*, з одного боку, якісна зміна особи злочинця та формування допоміжних технократичних сил, які виконують забезпечувальну функцію на окремих стадіях реалізації злочинних технологій; *по-п'яте*, формування цифрових кримінальних ринків.

Безумовно, що усі ці напрями знаходяться у системних зв'язках між собою, але зважаючи на особливості кожного з них, можуть бути досліджені відокремлено з подальшим узагальненням.

Так, першим напрямом взаємозв'язків є ***криміналізація окремих діянь, зумовлена широкомасштабним використанням кіберпростору у всіх сферах суспільного життя***. У контексті нашого дослідження слушно підтримати позицію Д.С. Азарова, який відзначає, що існування тих чи інших кримінально-правових норм не може зумовлюватись лише поширеністю тих чи інших посягань. Порівняно незначна кількість зареєстрованих у нашій країні суспільно небезпечних діянь у сфері комп'ютерної інформації не повинна істотно впливати на встановлення кримінальної відповідальності за їх вчинення. Насамперед необхідно враховувати характер і ступінь суспільної небезпеки означених діянь. Саме суспільна небезпека має розглядатись як головна підстава їх криміналізації (декриміналізації) [1; 16]. Саме тому, на нашу думку, незважаючи на незначну кількість зареєстрованих на початковому етапі освоєння кіберпростору громадянами нашої держави високотехнологічних злочинів, було вжито заходів щодо кримінально-правової охорони суспільних відносин, які пов'язані з використанням інноваційних форм представлення інформації та використанням комп'ютерної техніки. Аналіз чинного КК України свідчить, що найпоширеніші види протиправних діянь у цій сфері закріплено в окремому розділі Особливої частини КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Аналіз норм КК України свідчить, що, формуючи концепцію кримінально-правової протидії економічній злочинності, вітчизняний законодавець не пішов шляхом закріплення окремих норм кримінального закону щодо екологічних злочинів, які вчиняються за допомогою кіберпростору, а лише встановив використання електронно-обчислювальних машин як кваліфікуючу ознаку для окремих складів кримінальних правопорушень, зокрема шахрайства. Такий підхід, з одного боку, є виправданим, оскільки зростання кількості економічних злочинів, які можуть бути вчиненні за допомогою кіберпростору, призвело б до значного та необґрунтованого розширення складів кримінальних правопорушень. Водночас такий підхід не враховує підвищений рівень суспільної небезпеки злочинів, вчинених із використанням кіберпростору.

Необхідно звернути увагу, що, на нашу думку, із розвитком цифрових процесів та процедур в економіці України підхід законодавця щодо реагування на відповідні дії на рівні кримінального закону зазнає змін.

Другим напрямом взаємозв'язків є якісна трансформація інфраструктури економічної злочинності, що зумовлено перетворенням кіберпростору у невід'ємну складову частину економічних відносин. У контексті цього наголосимо, що вироблення ефективних організаційно-тактичних моделей виявлення злочинів неможливе без аналізу середовища функціонування злочинності як соціального явища, зокрема й легальних соціальних, економічних та технологічних структур, які можуть бути використаними для забезпечення кримінальної активності.

При цьому слушно звернути увагу, що сучасними вченими-криміналістами кіберпростір не розглядався крізь призму інфраструктури злочинності, а увага, у переважній більшості, акцентувалась на аналізі кіберпростору як: *по-перше*, обстановки вчинення злочину; *по-друге*, знаряддя вчинення злочину. Водночас, на нашу думку, таких науковий підхід є занадто спрощеним, адже виключає з поля зору ті елементи кіберпростору, які можуть використовуватись поза межами вчинення конкретного кримінального правопорушення чи реалізації складної технології злочинної діяльності. Так, на нашу думку, кіберпростір як складова частина інфраструктури економічної злочинності може виконувати такі функції:

1) *інтелектуальне та інформаційне забезпечення злочинної діяльності*. У контексті цього необхідно відзначити, що кіберпростір як відпо-

відний соціально-технологічний феномен не реалізує вказану функцію у формі безпосередньої активності, а є інформаційним ресурсом для отримання відповідних знань та компетенцій злочинцями, зокрема щодо: *по-перше*, особливостей технологічного здійснення відповідних фінансових операцій у віртуальному середовищі; *по-друге*, аналітичних узагальнень щодо недоліків окремих видів програмного забезпечення, технологічних циклів та окремих моделей фінансових транзакцій; *по-третє*, загальне підвищення інтелектуального рівня злочинців за рахунок узагальнення досвіду злочинної діяльності інших осіб; *по-четверте*, миттєве отримання інформації щодо появи програмних продуктів та інструкцій з їх використання, які можуть бути застосовані у злочинній діяльності;

2) *створення умов для формування стійких безконтактних зв'язків між особами, які в подальшому можуть здійснювати спільну злочинну діяльність*. Зважаючи на викладене, розвиток кіберпростору як інфраструктурного елемента злочинності призвів до появи злочинних угруповань «мережевого типу», для яких характерні такі ознаки: а) відсутність чітко вираженого лідера (лідером під час вчинення конкретного правопорушення є особа, яка розробила ідею його вчинення, що дозволяє будь-якому члену злочинного угруповання зайняти лідерську позицію під час реалізації конкретного епізоду злочинної діяльності); б) безконтактний спосіб функціонування таких груп, що виключає необхідність особистого знайомства, комунікації та використання особистих даних; в) можливість знаходження членів такого угруповання у різних юрисдикціях під час здійснення злочинної діяльності;

3) *забезпечення ринку збуту відповідних кримінальних послуг та кримінальних компетентностей*. Так, безумовно, як інфраструктурний елемент економічної злочинності кіберпростір володіє ознакою легальності, що унеможливлює вплив на його функціонування звичними для оперативних підрозділів прийомами та методами. Водночас невід'ємною складовою частиною кіберпростору як легальної структури став сегмент який, фактично, створений на його базі для систематичного та стійкого забезпечення злочинної діяльності – "Darknet". Darknet – це накладена мережа Інтернету, доступ до якої можна отримати лише за допомогою спеціалізованого програмного забезпечення, конфігурацій та спеціальних авторизацій, і часто використовує нестандартні протоколи зв'язку, щоб Інтернет навмисно був недоступним. Darknet стосується мереж, які не індексуються пошуковими системами, такими як Google, Yahoo або Bing. Це мережі, які доступні лише для вибраної групи людей, а не для широкої громадськості в Інтернеті, і доступні лише через авторизацію, певне програмне забезпечення та конфігурації. Це включає нешкідливі місця, такі як академічні бази даних та корпоративні сайти, а також ті, що мають більш темні теми, такі як чорні ринки, фетиш-спільноти, хакерство та піратство. Darknet відрізняється від інших розподілених мереж P2P, оскільки обмін даними є анонімним, і тому користувачі можуть спілкуватися не поза урядовим контролем чи корпоративним втручанням. З цієї причини Darknet часто асоціюється з політичними комунікаціями дисидентів та незаконною діяльністю. У більш загальному плані термін Darknet може бути використаний для опису всіх некомерційних веб-сайтів в Інтернеті або для позначення всіх «підпільних» веб-комунікацій та технологій, найчастіше пов'язаних з незаконною діяльністю. Технічно Darknet – це різновид віртуальної приватної мережі (VPN) з додатковими заходами, що забезпечують неможливість виявлення мережі та IP-адрес учасників. Мета полягає в тому, щоб приховати не тільки самі повідомлення, але і сам факт обміну інформацією. Учасники приєднуються з надією на можливість обмінюватися інформацією або файлами з невеликим ризиком виявлення.

Так, проведений нами контент-аналіз п'яти сайтів у мережі Darknet свідчить, що на момент аналізу на них було розміщено біля 400 оголошень: 1) близько 200 оголошень, присвячених продажу чи розповсюдженню наркотичних засобів чи психотропних речовин; 2) окремий розділ «Цифрові товари» містив 100 оголошень, на яких пропонували доступ до зламаних баз даних державних органів; 3) інша частина оголошень стосувалась можливості придбати документи на володіння транспортними засобами.

З викладеного вище витікає відособлена форма зв'язків між розвитком кіберпростору та злочинною діяльністю – ***поява цифрових кримінальних ринків***. Необхідно зауважити, що безумовно передумовою цього явища було створення та розвиток легальних цифрових (електронних) ринків, під якими можна розуміти систему економічних відносин у віртуальному просторі, які складаються між суб'єктами економічної діяльності щодо торгівлі послугами/товарами через інноваційні середовища створенні на базі високих інформаційних технологій. У свою чергу, форму-

вання електронних ринків вимагало нових підходів щодо здійснення фінансових операцій. Саме тому ми підтримуємо позицію науковців, які відзначають, що конвергенція комп'ютерних мереж зумовила і конвергенцію фінансових операцій; наприклад, до переліку електронних банківських операцій належать: операції з картковими рахунками; операції з переказу грошей без відкриття банківського рахунку; операції з управління електронним банківським рахунком (системи «клієнт-банк» з доступом через Інтернет); через комп'ютерні мережі здійснюється також низка операцій з оплатою: електронна комерція – створення віртуальних магазинів, реклама, продаж і проведення розрахунків засобами інформаційно-телекомунікаційних технологій (у тому числі платіжними картками); Інтернет-банкінг – здійснення через систему Інтернет міжбанківських операцій та обслуговування клієнтів; IP-телефонія – здійснення двостороннього голосового контакту через мережу Інтернет [2; 5].

Електронні ринки стали привабливими об'єктами для перетворення їх у складову частину інфраструктури економічної злочинності, оскільки вони характеризуються диверсифікацією цін, ціновою еластичністю, зменшенням витрат на сегментацію ринків тощо. Іншою вагомою причиною освоєння електронних ринків кримінальними структурами є постійний пошук шляхів підвищення «рентабельності» злочинної діяльності, що забезпечується: скороченням витрат на збут, «рекламу» і утримання роздрібної мережі; зменшенням витрат на зберігання товарів; оптимізацією системи забезпечення ресурсами. Крім того, електронний ринок підтримує координацію кримінальних зв'язків між злочинними угрупуваннями за рахунок оптимізації надійності та динамічності зв'язків; сприяє формуванню власного інформаційно-економічного простору.

Водночас поряд із легальними цифровими ринками, які активно освоюються кримінальними структурами, виникли і нові криміногенні феномени, зокрема цифрові кримінальні ринки. Загалом слушно звернути увагу, що питання протидії створенню та функціонуванню кримінальних ринків досліджувалось на шпальтах наукових видань. Водночас наявні наукові дослідження розглядають вказану проблему у контексті злочинної діяльності злочинних угруповань загальнокримінальної спрямованості, які формують та контролюють кримінальні ринки товарів та послуг на відповідних територіях, зокрема кримінальний ринок наркотиків, викрадених транспортних засобів, зброї тощо. Необхідно зауважити, що запропоновані вченими моделі щодо протидії функціонуванню таких кримінальних ринків не можуть бути екстрапольовані на цифрові кримінальні ринки, які потребують застосування інших моделей у контексті: *по-перше*, організації оперативного обслуговування; *по-друге*, виявлення усієї технології постачання та реалізації відповідних товарів на кримінальних ринках; *по-третє*, ідентифікації осіб, які здійснюють протиправну діяльність на таких ринках. Видається, що у даному випадку існує необхідність комплексного підходу, у тому числі й з використанням традиційних методів та засобів оперативно-розшукової діяльності.

Загалом, на нашу думку, під ***цифровими кримінальними ринками*** необхідно розуміти стійку, централізовано не контрольовану систему, яка здатна до самовідтворення і саморегуляції, спрямовану на створення з урахуванням структури та динаміки попиту пропозиції заборонених у цивільному обігу товарів та послуг у кіберпросторі.

Зважаючи на викладене, можна виокремити типові ознаки кримінальних ринків, які відрізняються від аналогічних утворень у фізичному просторі: *по-перше*, транснаціональний характер та можливість функціонування на таких ринках агентів із будь-якої юрисдикції; *по-друге*, високий рівень анонімності агентів таких ринків та підвищення рівня своєї активності за рахунок створення відповідної репутації на ринку; *по-третє*, можливість безконтактної передачі окремих видів товарів та послуг із використанням кіберпростору, наприклад окремих типів програмного забезпечення чи інших протиправних даних; *по-четверте*, використання специфічних інструментів оплати, зокрема криптовалютних та інших нетрадиційних засобів платежів.

Наразі одним із найвідоміших прикладів цифрового кримінального ринку є Hydra Market, який є нелегальним торгівельним майданчиком доступ, до якого надається через мережу Tor з 2015 року. Лише у 2020 році продажі на вказаному нелегальному ринку склали 1, 23 мільярди євро, а кількість клієнтів становила 17 мільйонів. Крім наркотиків, популярними товарами на цьому ринку були фальшиві гроші та документи, інструкції щодо здійснення протиправної діяльності, послуги з Інтернет-безпеки та злому аккаунтів.

Висновки. Частково підсумовуючи, можна відзначити, що розвиток кіберпростору перетворив його у самостійний елемент інфраструктури економічної злочинності. Аналіз практики роботи оперативних підрозділів свідчить, що переважній

більшості випадків у якості інфраструктурного елементу використовуються мережеві системи, які створенні із соціально-корисною метою. Крім того, опитування працівників оперативних підрозділів дозволяє зробити висновок, що декриміналізація мережі Інтернет, у тому числі мінімізація можливостей її використання як складової інфраструктури злочинності вимагає: формування правової основи здійснення фінансових, податкових та господарських операцій через мережу Інтернет; розроблення інституційної основи контролю за національним сегментом мережі Інтернет; розроблення принципів, тактичних прийомів та належного кадрового забезпечення оперативного обслуговування національного сегменту мережі.

Література

1. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : монографія. Київ : Атіка, 2007. 304 с.

2. Комар О.М. Протидія оперативними підрозділами МВС України шахрайствам, вчинюваним шляхом незаконних операцій з використанням електронно-обчислювальної техніки : автореф. дис…. канд. юрид. наук : 12.00.09. Київ, 2013. 20 с.

3. Панченко О.А., Гнатенко В.С. Економічна безпека в державній системі національної безпеки. *Публічне урядування*. 2021. № 2. С. 22–31.

4. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія. Одеса : Юридична література, 2011. 216 с.

5. Цифрова економіка: тренди, ризики та соціальні детермінанти. Київ : Вид-во «Заповіт», 2020. 274 с.

Куліуш В.М.,
аспірант кафедри кримінального процесу
Одеського державного університету внутрішніх справ