УДК 343.9
DOI https://doi.org/10.32782/pdu.2022.3.61

І. І. Липкан
здобувач
Науково-дослідного інституту публічного права,
ORCID ID: 0009-0000-6685-2650

ПОНЯТТЯ ВІРТУАЛЬНОГО ПРОСТОРУ ЯК СЕРЕДОВИЩА ДЛЯ ВЧИНЕННЯ КІБЕРШАХРАЙСТВ

У статті розглянуто поняття та сутність віртуального простору як середовища, де вчиняється кібершахрайство. Доведено, що інтернет-простір можна трактувати як платформу, де здійснюється глобальний обмін інформацією між індивідами, організаціями, державами. Це середовище не обмежується лише технічними аспектами (наприклад, мережею серверів чи протоколами зв'язку), а включає соціальні, культурні та економічні зв'язки, що утворюються в процесі використання інтернет-ресурсів. Інтернет стає не лише способом передавання даних, але й умовою виникнення нових форм комунікації, культурних явищ, спільнот, а також нових типів кримінальних правопорушень. Встановлено, що на сьогодні в Україні ще не сформовано єдиний понятійний апарат щодо середовища, в якому вчиняються кримінальні правопорушення, пов'язані з використанням цифрових технологій. Однак, це не є критичною проблемою, оскільки в науковій літературі часто існує консенсус щодо ототожнення понять «кіберпростір», «віртуальний простір» і «інформаційний простір», що дозволяє вільно застосовувати їх у контексті дослідження злочинності, пов'язаної з цифровими технологіями. Ми підтримуємо науковців у тому, що «мережа Інтернет» є більш конкретним поняттям і однією з основних складових кіберпростору. Враховуючи те, що Інтернет є важливим інструментом для злочинців, що здійснюють шахрайства та інші правопорушення в онлайн-просторі, використання терміну «мережа Інтернет» для опису саме цих порушень є доцільним. Для зменшення можливостей для шахрайства в електронній комерції запропоновано: 1) посилити вимоги до ідентифікації користувачів платіжних систем, зокрема зобов'язати їх надавати більше інформації про свої особисті дані; 2) контролювати анонімні транзакції через електронні платіжні системи, зокрема через введення правил, які вимагають певного рівня верифікації користувачів перед проведенням транзакцій; 3) забезпечити інтеграцію з правоохоронними органами, адже платіжні системи мають співпрацювати з державними органами для швидкого реагування на випадки шахрайства; 4) створення чітких правил для електронної комерції, оскільки для інтернет-магазинів та інших учасників ринку потрібно чітко визначити законодавчі вимоги щодо фінансових операцій та захисту споживачів від зловживань.

Ключові слова: *кібершахрайство, шахрайство у сфері цифрових технологій, незаконні транзакції, кримінальне правопорушення, доказування.*

Постановка проблеми. Кримінальні правопорушення, пов'язані з використанням цифрових технологій, неможливі без існування певного віртуального простору, де ці кримінальні правопорушення вчиняються. Однак стрімкий розвиток інформаційно-комунікаційних технологій призвів до суттєвого розширення й трансформації самого поняття «віртуальний простір». Це поняття стало широко вживаним і його інтерпретація набуває різноманітних смислових відтінків залежно від контексті [1, с. 163–170].

Аналіз наукової літератури показує, що термін «віртуальний простір» часто замінюється іншими поняттями, такими як «інтернет-простір», «кіберпростір», «інформаційний простір», «віртуальний світ» тощо. Це викликає питання щодо їх синонімічності або, навпаки, різного значення, оскільки кожне з цих понять може мати своє власне трактування в різних сферах.

Метою наукової статті є вивчення поняття та сутності віртуального про-

стору як середовища, де вчиняються шахрайства з використанням цифрових технологій.

Виклад основного матеріалу. Більшість фахівців погоджуються з тим, що інтернет-простір є невід'ємною складовою інформаційного простору. Він не лише забезпечує засоби обміну соціальною інформацією, а й стає носієм специфічної культури, яка виникає у результаті взаємодії користувачів у віртуальному середовищі [2, с. 346–349].

Інтернет-простір можна трактувати як платформу, де здійснюється глобальний обмін інформацією між індивідами, організаціями, державами. Це середовище не обмежується лише технічними аспектами (наприклад, мережею серверів чи протоколами зв'язку), а включає соціальні, культурні та економічні зв'язки, що утворюються в процесі використання інтернет-ресурсів. Інтернет стає не лише способом передавання даних, але й умовою виникнення нових форм комунікації, культурних явищ, спільнот, а також нових типів кримінальних правопорушень.

На думку О.О. Кіпи, віртуальний простір можна розглядати як складну модель, що існує завдяки комп'ютерним технологіям. Цей простір являє собою інформаційну мережу, де зберігаються та передаються дані про осіб, об'єкти, явища, події та процеси. Віртуальний простір характеризується тим, що ці дані можуть бути представлені в різних формах – від математичних моделей і символьних виразів до інших форматів інформації, що зберігаються або передаються через локальні й глобальні комп'ютерні мережі [2, с. 164].

Основні характеристики цього віртуального простору, згідно з думкою науковця, включають:

1) моделювання інформації, оскільки віртуальний простір складається з даних, які можуть бути представлені в різних математичних, символьних або інших формах.

2) динамічний процес, адже дані в цьому просторі перебувають у постійному русі через мережі або зберігаються на різних фізичних або віртуальних пристроях.

3) інформаційні носії: це можуть бути фізичні пристрої, як комп'ютери чи сервери, або віртуальні носії, спеціально призначені для зберігання, обробки та передачі інформації [2].

О. Ткаченко та Т. Ткаченко наводять різні підходи до формалізації поняття «кіберпростір», які мають своєрідні акценти залежно від аспекту, що розглядається. До них належать:

1) кіберпростір як середовище взаємодії – це концепція, в рамках якої кіберпростір визначається як середовище, що виникає завдяки взаємодії людей, програмного забезпечення та інтернет-послуг, що здійснюються через технологічні пристрої і мережі, під'єднані до цих пристроїв. Тут підкреслюється абстрактність кіберпростору, адже він не має фізичної форми, але є важливим для взаємодії учасників віртуального середовища.

2) кіберпростір як сфера обміну даними – у цьому підході кіберпростір визначається як простір, що забезпечує використання електронних і електромагнітних засобів для запам'ятовування, модифікації та обміну даними через різні системи. Тут акцент робиться на технологічні процеси, що відбуваються в ньому.

3) кіберпростір як цифрова активність – цей підхід розглядає кіберпростір як включення всіх форм мережної та цифрової активності, що охоплює контент та дії з його обробки. Така перспектива підкреслює динамізм і взаємодію цифрових об'єктів у мережі.

4) кіберпростір як інфраструктура, доступна через інтернет – це визначення акцентує увагу на інфраструктурі, яка забезпечує доступ до інформаційних ресурсів через інтернет, що є важливим для обміну та зберігання даних.

5) кіберпростір як комунікаційне середовище – тут кіберпростір описується як система зв'язків між різними об'єктами кіберінфраструктури, включаючи комп'ютерні мережі, електронні обчислювальні машини, програмне забезпечення та інформаційні ресурси. Цей підхід орієнтований на розуміння кіберпростору як інтеграції різних технічних і програмних елементів, що забезпечують комунікацію між об'єктами [3, с. 75–86].

В.М. Фурашев визначає кіберпростір як специфічну форму співіснування

матеріальних і нематеріальних об'єктів і процесів, які мають на меті породжувати, сприймати, зберігати, переробляти та обмінювати інформацію. Згідно з його концепцією, кіберпростір охоплює весь спектр інформаційних процесів, що здійснюються за допомогою різноманітних технологій і пристроїв, призначених для обробки та передачі даних.

Науковець справедливо стверджує, що поняття «кіберпростір» та «інформаційний простір» є тотожними за своєю сутністю, хоча різні науковці можуть використовувати їх як окремі терміни. В його погляді, застосування будь-якого з цих понять не змінює самого процесу або явища, а може лише спричинити термінологічну плутанину, оскільки обидва ці терміни описують одну й ту ж саму реальність – простір для циркуляції інформації, в який входять як цифрові, так і традиційні форми інформаційних комунікацій [4, с. 162–175].

Питання визначення поняття «Інтернет» залишається проблематичним у правовому полі, оскільки ані в міжнародному праві, ані в національних законодавствах немає єдиного розуміння цього терміна. Як зазначає С.Ф. Гуцу, відсутність чіткого законодавчого визначення Інтернету створює правову невизначеність, зокрема у сфері кіберзлочинності [5, с. 114–118].

У науковій літературі також існують різні підходи до розуміння природи Інтернету, оскільки це поняття охоплює широкий спектр технологій і сервісів, які постійно змінюються. Зокрема, Інтернет можна розглядати як глобальну систему комп'ютерних мереж, що дозволяє користувачам обмінюватися інформацією в різних форматах, але існують й інші трактування, що включають в себе різні аспекти: технічний, соціальний і навіть правовий.

У зв'язку з цим, різні науковці та практики пропонують різні визначення Інтернету в контексті кіберзлочинності, але всі вони сходяться на тому, що Інтернет є потужним засобом як для здійснення правомірних дій, так і для вчинення кримінальних правопорушень. Це ускладнює розробку чітких та ефективних правових норм для боротьби з кіберзлочинністю, оскільки відсутність єдиного визначення Інтернету перешкоджає виробленню універсальних підходів у правовому регулюванні кіберзлочинів.

Отже, на сьогодні в Україні ще не сформовано єдиний понятійний апарат щодо середовища, в якому вчиняються кримінальні правопорушення, пов'язані з використанням цифрових технологій. Однак, це не є критичною проблемою, оскільки в науковій літературі часто існує консенсус щодо ототожнення понять «кіберпростір», «віртуальний простір» і «інформаційний простір», що дозволяє вільно застосовувати їх у контексті дослідження злочинності, пов'язаної з цифровими технологіями. Ми підтримуємо науковців у тому, що «мережа Інтернет» є більш конкретним поняттям і однією з основних складових кіберпростору. Враховуючи те, що Інтернет є важливим інструментом для злочинців, що здійснюють шахрайства та інші правопорушення в онлайн-просторі, використання терміну «мережа Інтернет» для опису саме цих порушень є доцільним.

Як зазначають вчені, на сьогодні продаж товарів у віртуальному просторі охоплює понад 20 мільйонів користувачів [6, с. 153–155].

Це справді вражаючий показник, що підкреслює зростання популярності електронної комерції в Україні. З огляду на цей факт, можна стверджувати, що Інтернет став не лише каналом для взаємодії між підприємствами та споживачами, а й важливою складовою економічної діяльності в країні. 20 мільйонів користувачів – це суттєва частка населення, що активно користується інтернетом для здійснення покупок і взаємодії з різними підприємствами, що працюють у сфері онлайн-продажів.

Для зменшення можливостей для шахрайства в електронній комерції науковці пропонують:

1) посилити вимоги до ідентифікації користувачів платіжних систем, зокрема зобов'язати їх надавати більше інформації про свої особисті дані;

2) контролювати анонімні транзакції через електронні платіжні системи, зокрема через введення правил, які вимагають певного рівня верифікації користувачів перед проведенням транзакцій;

3) забезпечити інтеграцію з правоохоронними органами, адже платіжні сис-

теми мають співпрацювати з державними органами для швидкого реагування на випадки шахрайства;

4) створення чітких правил для електронної комерції, оскільки для інтернет-магазинів та інших учасників ринку потрібно чітко визначити законодавчі вимоги щодо фінансових операцій та захисту споживачів від зловживань.

Отже, професійне шахрайство дійсно є глобальною проблемою, і боротьба з ним стає важливим аспектом правоохоронної діяльності в усіх країнах світу. Водночас варто відзначити, що хоча конкретні результати боротьби з шахрайством можуть змінюватися в залежності від країни, загальні тенденції та схеми шахрайських дій мають багато спільного в різних регіонах. Зловживання, пов'язані з фінансовими махінаціями, а також їхня легалізація (відмивання незаконно отриманих доходів), є частими супутниками таких кримінальних правопорушень.

Одним із ключових завдань правоохоронних органів є розробка та впровадження ефективних технологій розслідування шахрайських схем, що включають в себе відмивання коштів. Ці схеми можуть бути складними, і від їх виявлення залежить не лише боротьба з економічними злочинами, а й забезпечення стабільності фінансової системи.

Для цього необхідно активно застосовувати різноманітні механізми, що дозволяють відстежувати рух незаконних коштів, включаючи фінансові технології і аналітичні інструменти. Одним із важливих аспектів є застосування заходів щодо своєчасного арешту активів, що дозволяє заморозити незаконно отримані кошти до того, як вони будуть легалізовані або використані злочинцями.

Щоб зменшити ймовірність шахрайських дій, підприємствам і організаціям доцільно зміцнювати внутрішній контроль та впроваджувати незалежний аудит. Важливо також оптимізувати та вдосконалювати наглядові функції, щоб своєчасно виявляти та запобігати можливим зловживанням.

Покращення цих систем дозволяє не лише знизити ймовірність шахрайства, але й покращити загальну прозорість фінансових операцій, що є важливим для розвитку здорової економічної середовища.

Отже, віртуальний простір, як середовище для здійснення різноманітних правочинів, потребує чітких і детальних правових норм. Через швидкий розвиток електронної комерції, використання новітніх технологій, а також складність визначення юрисдикції у трансакціях через Інтернет, існують численні прогалини в законодавстві. Ці прогалини можуть призводити до зловживань, зокрема шахрайських схем, і ускладнювати захист прав споживачів.

Список використаних джерел:

1. Дзьобань О.П. Сучасний віртуальний простір: конгеніальність віртуальності й міфу. *STRATEGICPRIORITIES*. № 3 (44), 2017. С. 163–170.
2. Кіпа О.О. Правопорушення в мережі «Інтернет». *Часопис Київського університету права*. 2010. № 4. С. 346–349
3. Ткаченко О., Ткаченко Т. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018. № 1. С. 75–86
4. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інфор- маційна безпека: сутність, визначення, відмінності. *Інформація і право*. № 2(5)/2012. С. 162–175.
5. Гуцу С.Ф. Правове регулювання мережі «Інтернет»: міжнародний і вітчизняний досвід. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. Випуск 2 (38) 2018. С. 114–118.
6. Мізерак А.Б. Шахрайство при інтернет-торгівлі: схеми та аспекти запобігання. *Маркетинг і контролінг: сучасні виклики підприємництв*. Київ, 2017. С. 153–155.

Lypkan I. I. The concept of virtual space as an environment for committing cyber fraud

The article examines the concept and essence of virtual space as an environment where cyber fraud is committed. It is proved that the Internet space can be interpreted as a platform for global exchange of information between individuals, organisations and states. This environment is not limited to technical aspects (e.g., a network of servers or

communication protocols), but includes social, cultural and economic ties formed in the process of using Internet resources. The Internet is becoming not only a means of data transmission, but also a condition for the emergence of new forms of communication, cultural phenomena, communities, and new types of criminal offences. It is established that today in Ukraine there is no unified conceptual framework regarding the environment in which criminal offences related to the use of digital technologies are committed. However, this is not a critical problem, since there is often a consensus in the scientific literature on the identification of the concepts of «cyberspace», «virtual space» and «information space», which allows them to be freely applied in the context of studying digital-related crime. We support scholars that the 'Internet' is a more specific concept and one of the main components of cyberspace. Given that the Internet is an important tool for criminals committing fraud and other offences in the online space, the use of the term 'Internet' to describe these offences is appropriate. To reduce opportunities for fraud in e-commerce, it is proposed to: 1) to strengthen the requirements for identification of payment system users, in particular, to oblige them to provide more information about their personal data; 2) to control anonymous transactions through electronic payment systems, in particular, by introducing rules requiring a certain level of user verification before transactions; 3) to ensure integration with law enforcement agencies, since payment systems should cooperate with government agencies to respond quickly to fraud cases; 4) establishing clear rules for e-commerce, as online retailers and other market participants need to clearly define legal requirements for financial transactions and protect consumers from abuse.

Key words: *cyber fraud, digital fraud, illegal transactions, criminal offence, proving.*