***УДК 343.9***
***DOI https://doi.org/10.24144/2788-6018.2023.02.49***

# КРИМІНАЛІСТИЧНА ТИПОЛОГІЗАЦІЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ

**Думчиков М.О.**
*кандидат юридичних наук, старший викладач кафедри кримінально-правових дисциплін та судочинства ННІ права Сумського державного Університету*
*https://orcid.org/ 0000-0002-4244-2419*

**Думчиков М.О. Криміналістична типологізація кримінальних правопорушень у кіберпросторі.**

Сьогодні злочинність у кібернетичному просторі, оголошена глобальною міжнародною проблемою, про що свідчать, як міжнародні домовленості, які передбачають спільні кроки до боротьби з цим високотехнологічним та технічним феноменом так і власне застосування різними країнами методів кібершпигунства та кібертероризму. При цьому, небезпеку від кримінальних правопорушень, які вчиняються у кіберпросторі визнають і правоохоронні органи різних держав світу. Наразі злочинність у кіберпросторі виступає однією з основних загроз національної безпеки і оборони України. Минулий рік, став певним каталізатором вироблення нових тактико-орієнтовних методів боротьби з кримінальними правопорушеннями у кіберпросторі, як в рамках суспільних відносин у сфері національної безпеки так і в інших сферах, зокрема безпечного функціонування цифрових пристроїв.

Здійснення правильної типологізації кримінальних правопорушень які вчиняються у кіберпросторі набуває не аби якого значення при правильному розслідуванні цього типу кримінальних правопорушень, та вироблення правильної методики збирання доказової бази.

В науковій роботі нами досліджено декілька підстав, щодо типологізації кримінальних правопорушень у кіберпросторі, зокрема: 1) Конвенції «Про кіберзлочинність»; 2) криміналістичної значимості елементів інформаційно-телекомунікаційних технологій; 3) за способами вчинення цього типу суспільно небезпечних діянь; 4) кваліфікації суб'єктів вчинення кримінальних правопорушень у кіберпросторі; 5) відповідно до об'єктів злочинного зазіхання.

Наголошується, що вивчення кримінальних правопорушень, які вчиняються у кіберпросторі в розрізі їх криміналістичного розуміння повинно мати комплексний характер і має розглядатися з різних сторін.

Встановлено, що у ході типологізаційного дослідження суспільно небезпечних діянь, які вчиняються у кіберпросторі не можна обмежуватися розподілом криміналістичної типологізації лише з однієї підстави, суть питання зобов'язує будувати типологізаційні системи за всіма можливими справжніми ознаками.

**Ключові слова:** кримінальні правопорушення у кіберпросторі, кіберзлочини, кіберзлочинність, класифікація кіберзлочинів, типологізація кіберзлочинів.

**Dumchykov M.O. Forensic typology of criminal offenses in cyberspace.**

Today, crime in the cyberspace has been declared a global international problem, as evidenced by international agreements that provide for joint steps to combat this high-tech and technical phenomenon, as well as the actual use of cyberespionage and cyberterrorism methods by various countries. At the same time, the danger from criminal offenses committed in cyberspace is also recognized by law enforcement agencies of various countries of the world. Currently, crime in cyberspace is one of the main threats to the national security and defense of Ukraine. The past year became a certain catalyst for the development of new tactical-oriented methods of combating criminal offenses in cyberspace, both within the framework of public relations in the field of national security and in other areas, in particular, the safe functioning of digital devices.

Carrying out the correct typology of criminal offenses committed in cyberspace is of great importance in the correct investigation of this type of criminal offences, and the development of the correct methodology for collecting the evidence base.

In our scientific work, we investigated several grounds for the typology of criminal offenses in cyberspace, in particular: 1) Convention «On Cybercrime»; 2) forensic significance of elements of information and telecommunication technologies; 3) by the methods of committing this type of socially dangerous acts; 4) qualifications of subjects who commit criminal offenses in cyberspace; 5) according to the objects of criminal encroachment.

It is emphasized that the study of criminal offenses committed in cyberspace in terms of their criminological understanding should have a complex

nature and should be considered from different angles.

It has been established that in the course of typological research of socially dangerous acts committed in cyberspace, one cannot be limited to the distribution of criminalistic typology on only one basis, the essence of the matter obliges to build typological systems based on all possible real signs.

**Keywords:** criminal offenses in cyberspace, cybercrimes, cybercrime, classification of cybercrimes, typology of cybercrimes.

**Постановка проблеми.** Результативність розслідування кримінальних правопорушень у кіберпросторі значною мірою залежить від характеру та обсягу інформації, якою володіє слідчий на початковому етапі слідчих дій. Віднесення кримінальних правопорушень до певного типологізаційного виду, значно полегшує вибір методики розслідування того чи іншого суспільно небезпечного діяння у кіберпросторі. Сьогодні в доктринальних джерелах визначені лише загальні риси типологізації кримінальних правопорушень, без виділення їх за об'єктами або предметами посягання.

**Стан опрацювання цієї проблематики.** Різні аспекти питання криміналістичної типологізації кримінальних правопорушень у кіберпросторі не втрачають своєї актуальності протягом останніх років та були предметом дослідження таких науковців як: Адамова О.С., Кравцов І.В., Шепітько Ю.В. та Дзюндзюк В.Б.

**Мета статті:** є здійснення криміналістичної типологізації кримінальних правопорушень у кіберпросторі на основі дослідження об'єкта, суб'єкта та предмета кримінального правопорушення.

**Виклад основного матеріалу.** Здійснюючи криміналістичну типологізації суспільно небезпечних діянь вчинених у кіберпросторі, хочемо почати з визначення сутності поняття криміналістична типологізація та власне типологізація загалом. О.С. Адамова під типологізацією розуміє, певну категорію, яка відбиває очевидне і зрозуміле кожному, однак в той же час є надзвичайно насиченою та неоднозначною. Зауважимо, що автор визначає типологізацію з точки зору філософського аспекту [1, с. 19].

В свою чергу І.В. Кравцов надає поняття саме правової типологізації, під якою розуміє, зокрема, як особливий метод, грамотне використання якого значно підвищує ефективність правового регулювання. Крім того на думку науковця правова типологізація може визначатися, як особливий прийом законодавчої техніки, правильне застосування якого буде сприяти вдосконаленню нормативно правових актів, і як результат вдосконалення правового регулювання суспільних відносин [2, с. 52].

Що стосується власне криміналістичної типологізації, то на думку Шепітько В.Ю., вона виступає певним провідником у пізнанні самого об'єкта, є невід'ємним засобом проникнення в його сутнісну складову та забезпечує виявлення певних закономірностей, які необхідні дня його наукового обґрунтування та опису [3].

На нашу думку криміналістична типологізація кримінальних правопорушень сьогодні набула найбезпосереднішого та найактивнішого практичного застосування в ході здійснення слідчої діяльності. Перш за все вона забезпечує правильне розуміння суті подій, які розслідуються, а також допомагає грамотно вибудувати, вибрати та застосувати запропоновані практиками криміналістичні методики розслідування окремих кримінальних правопорушень у кіберпросторі.

На нашу думку найбільш повною є типологізація кримінальних правопорушень у кіберпросторі на основі положень Будапештської Конвенції «Про кіберзлочинність». Сьогодні, типологізація на основі зазначеної Конвенції справедливо можна вважати еталонною. Відповідно до Конвенції всі кримінальні правопорушення, які можуть вчинятися у кібернетичному просторі варто ділити на п'ять груп: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з комп'ютерами; 3) правопорушення, пов'язані зі змістом; 4) правопорушення, пов'язані з порушенням авторських та суміжних прав; 5) правопорушення, зафіксовані в окремому протоколі, – це акти расизму та ксенофобії, скоєні з використанням комп'ютерних мереж [4].

У криміналістичної типологізації кримінальних правопорушень у кіберпросторі Дзюндзюк В.Б. зазначає основні криміналістично значимі елементи цього виду суспільно небезпечних діянь та його взаємні відносини вкладеності і підзвітності [5].

За способами вчинення кримінальні правопорушення у кіберпросторі можна типологізувати на: 1) неправомірне підключення до інформаційно – телекомунікаційних систем та мереж; 2) створення, використання, розповсюдження та збут мережевого шкідливого програмного забезпечення; 3) протиправне створення, використання, розповсюдження або збут, матеріалів заборонених до публічного і вільного обороту, вчиненого шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж; 4) порушення авторських та суміжних прав в мережі Інтернет; 5) шахрайство вчинене з використанням цифрових пристроїв; 6) крадіжка вчинена в кібернетичному просторі; 7) надання комерційних послуг в мережі Інтернет без оформлення фізичної особи підприємця; 8) вимагання у кіберпросторі; 9) кібертероризм.

В свою чергу С.В. Еміліо пропонує наступну типологізацію кримінальних правопорушень у кіберпросторі, яка основана на цілі вчинюваного

суспільно небезпечного діяння у кіберпросторі: 1) кримінальні правопорушення в яких елементи інформаційно-телекомунікаційних технологій є основним об'єктом кримінального правопорушення, наприклад порушення встановленого порядку маршрутизації цифрової інформації; 2) кримінальні правопорушення в яких елементи інформаційно-телекомунікаційних технологій виступають проміжною метою, тобто коли за допомогою інформаційно-телекомунікаційних технологій вчиняються інші суспільно небезпечні діяння; 3) кримінальні правопорушення в яких елементи інформаційно-телекомунікаційних технологій виступають лише автоматизованим засобом суспільно небезпечного, протиправного діяння; 4) кримінальні правопорушення в яких елементи інформаційно-телекомунікаційних технологій виступають засобом забезпечення злочинної діяльності [6].

Найбільш поширеною типологізацією, яка зустрічається в доктринальних джерелах виступає типологізація на основі об'єкту посягання відповідно до розділів Особливої частини Кримінального кодексу України. Сьогодні, коли процеси діджиталізації та цифровізації розвиваються набагато швидше за усі інші, коли ареною венних дій виступає не лише повітря, море та суходіл, але й кібернетичний та інформаційний простори, можна в упевненістю говорити, що об'єктом кримінальних правопорушень у кіберпросторі можуть виступати, як відносини пов'язані з національною безпекою держави, так і відносини в сфері власності.

В свою чергу кримінальні правопорушення у кіберпросторі за предметом посягання можна умовно поділити: 1) суспільно небезпечні діяння які мають матеріальний предмет посягання; 2) суспільно небезпечні діяння, які не мають матеріального предмету посягання. До першої групи можна віднести різного роду предмети матеріального світу, речі при вчиненні шахрайства у соціальних мережах або на маркетплейсах. До другої групи прийнято відносити цифрову інформацію, віртуальні активи та електронні гроші.

К. Джонатан в основу криміналістичної типологізації кримінальних правопорушень у кіберпросторі бачить у проведенні аналізу об'єкта злочинного зазіхання – цифрової інформації як складного багаторівневого об'єкта, та виявлення набору елементарних операцій на кожному його рівні. Наслідуючи свою позицію, науковець виділяє такі види кримінальних правопорушень цього типу: 1) знищення (руйнування) цифрової інформації; 2) неправомірне заволодіння цифровою інформацією чи порушення виключного права її використання; 3) неправомірне заволодіння цифровою інформацією як сукупністю відомостей, документів – порушенням виключного права володіння; 4) неправомірне заволодіння цифровою інформацією як алгоритмом (методом) її перетворення; 5) неправомірне оволодіння цифровою інформацією як товаром; 6) дії або бездіяльність щодо створення (генерації) цифрової інформації із заданими властивостями; 7) розповсюдження телекомунікаційними каналами інформаційно-обчислювальних мереж цифрової інформації, що завдає шкоди абонентам; 8) розробка та розповсюдження комп'ютерних вірусів та інших шкідливих програм для цифрових пристроїв; 9) неправомірна модифікація цифрової інформації; 10) неправомірна модифікація цифрової інформації як сукупності фактів, відомостей; 11) неправомірна модифікація цифрової інформації як алгоритм [7].

Залежно від кваліфікації суб'єктів вчинення кримінальних правопорушень у кіберпросторі ми виділити наступні типологізаційні групи: 1) професійні користувачі – це фахівці, для яких інформаційно-телекомунікаційні технології є предметом діяльності, або засобом та умовою діяльності, або інструментом для вирішення професійних завдань; 2) непрограмуючі користувачі – це люди, які використовують готові програмні продукти, що не потребують навичок програмування; 3) випадкові користувачі – це дилетанти, які стикаються з комп'ютером уперше і здатні користуватися лише елементарними програмними продуктами.

Вивчення кримінальних правопорушень, які вчиняються у кіберпросторі в розрізі їх криміналістичного розуміння повинно мати комплексний характер і підлягатиме розгляду з різних сторін, у різних зрізах. У ході типологізаційного дослідження суспільно небезпечних діянь, які вчиняються у кіберпросторі не можна обмежуватися розподілом криміналістичної типологізації лише з однієї підстави, суть питання зобов'язує будувати типологізаційні системи за всіма можливими справжніми ознаками.

Типологізація кримінальних правопорушень у кіберпросторі також можлива за ознаками процесу розслідування, зокрема, розслідування кримінальних правопорушень у сприятливих чи несприятливих умовах слідчих ситуацій. З урахуванням організації поетапного проведення слідчих дій кримінального правопорушення, що розслідуються як в умовах сприятливих, так і несприятливих ситуацій, логічно поділити на дві групи: 1) розслідувані у відповідних ситуаціях, що складаються на початковому етапі роботи у кримінальній справі; 2) розслідувані у відповідних ситуаціях, що складаються надалі.

Визначені у статті варіанти типологізації кримінальних правопорушень у кіберпросторіє передумовою для розробки завдань, засобів та методів, які можна використовувати під час розслідування кримінальних правопорушень (зокрема, спеціальних техніко-криміналістичних засобів та методів виявлення та дослідження різних специфічних матеріальних об'єктів, типізації та систематиза-

ції кримінальних та криміналістичних ситуацій). Формування теорії криміналістичної типологізації кримінальних правопорушень у кіберпросторі стане серйозним внеском у загальну методологію криміналістики як систему світоглядних принципів, концепцій, категорій, понять, методів боротьби зі злочинністю.

З практичної точки зору значимість криміналістичної типологізації суспільно небезпечних діянь у кіберпросторі обумовлена її логічним змістом, апробацією комплексу типових слідчих версій у кримінальній справі, що є надійною гарантією всебічності та повноти розслідування кримінальних правопорушень цього типу.

Подальша розробка теоретичних основ криміналістичної типологізації кримінальних правопорушень у кіберпрострі стане актуальним науковим завданням, обумовленим потребами криміналістичної теорії та практики виявлення та розслідування суспільно небезпечних діянь цього типу.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**

1. Адамова О.С. Поняття правової класифікації. Часопис цивілістики. Випуск 18. С. 19–22.
2. Кравцов І.В. Класифікація правових цінностей та її значення для правової теорії і практики. Наукові записки НаУКМА. 2017. Том 200. Юридичні науки. С. 51–55.
3. В.Ю. Шепітько, В.О. Коновалова, В.А. Журавель. Криміналістика. 2010. URL: https://sci-book.com/kriminalistika-pidruchniki/kriminalistika6533.html.
4. Про кіберзлочинність: Конвенція від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.
5. Дзюндзюк В.Б. Поява і розвиток кіберзлочинності. Державне будівництво. 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3.
6. Emilio C. Viano. Cybercrime: Definition, Typology, and Criminalization. URL: https://www.researchgate.net/publication/311584382_Cybercrime_Definition_Typology_and_Criminalization/references.
7. Jonathan Clough. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. URL: https://www.researchgate.net/publication/225469687_Data_Theft_Cybercrime_and_the_Increasing_Criminalization_of_Access_to_Data.