

ХАРАКТЕРИСТИКА КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

CHARACTERISTICS OF CRIMINAL OFFENSES IN THE SPHERE OF THE USE OF DIGITAL TECHNOLOGIES

Бенескул А.В., аспірант

Державного податкового університету

ORCID ID: 0009-0004-5315-3374

У статті досліджуються кримінальні правопорушення у сфері використання цифрових технологій. Автор наголошує на тому, що загальна цифровізація, діджиталізація та інформатизація суспільства значно загострила проблематику злочинності у сфері цифрових технологій та потребує належного вирішення і правового врегулювання. Небезпека таких кримінальних правопорушень обумовлена не лише масштабами згубних впливів, наприклад, результатами посягань на критично важливі та потенційно небезпечні інформаційні інфраструктури, а й зростанням їхньої кількості. Сьогодні з розвитком цифрових технологій значно збільшується і кількість правопорушень у сфері цифрової інформації та цифрових технологій загалом. Незважаючи на громадську небезпека подібних діянь, у теорії та практиці використання інформаційно-комунікаційних та цифрових технологій у злочинних цілях в останні роки, як і раніше, є серйозним викликом як для правоохоронних, так і та законодавчих органів. Жертвами кримінальних правопорушень, вчинених з використанням інформаційно-комунікаційних та цифрових технологій, щорічно стає багато людей та організацій, а також органи влади. Кіберзлочинність продовжує створювати економічні, безпекові та технологічні проблеми для розвинених і менш розвинених країн. Суспільство та держави все більше залежать від цифровізації та інформаційних комунікацій, цифрових технологій, що в свою чергу підвищує і ймовірність кіберзлочинності. Автор пропонує під кримінальними правопорушеннями у сфері цифрових технологій розуміти передбачене кримінальним законом винне, протиправне, суспільно небезпечне діяння, спрямоване на порушення конфіденційності, цілісності, достовірності та доступності цифрової інформації, що охороняється законом або вчинене з використанням цифрових технологій або щодо них. У статті відмічається, що стрімкий розвиток сфери цифрових технологій постійно призводить не лише до появи нових видів послуг у фінансовій сфері, а й вдосконаленню способів та методів незаконного отримання коштів у кіберсередовищі. Значної шкоди завдають кримінальні правопорушення у цифровому середовищі бізнесу, тобто, юридичним особам, для яких вже стали критичними втрати від кібератак на фінанси. Практично неможливо оцінити справжні масштаби негативних наслідків від цифрової злочинності, оскільки не всі жертви завжди усвідомлюють та розуміють, що вони стали жертвами таких кримінальних правопорушень і неможливо точно визначити реальну кількість потерпілих від, наприклад фішингових чи хакерських атак тощо. Саме тому, існуюча правова база боротьби з цифровою злочинністю та інші антикримінальні інструменти впливу потребують вдосконалення. Саме тому, автор пропонує зміни та доповнення до кримінального законодавства з метою врегулювання досліджуваного питання.

Ключові слова: злочинність, комп'ютерна злочинність, кримінальне законодавство, цифровізація, цифрові технології, запобігання злочинності, цифрова інформація, цифрова злочинність.

The article examines criminal offenses in the field of using digital technologies. The author emphasizes that the general digitization, digitization and informatization of society has significantly exacerbated the problem of crime in the field of digital technologies and requires proper resolution and legal regulation. The danger of such criminal offenses is determined not only by the scale of harmful effects, for example, the results of encroachments on critically important and potentially dangerous information infrastructures, but also by the growth of their number. Today, with the development of digital technologies, the number of offenses in the field of digital information and digital technologies in general is increasing significantly. Despite the public danger of such acts, there is no unified definition of the analyzed criminal offenses in theory and practice. Despite the rather frequent discussion of this issue, the use of information, communication and digital technologies for criminal purposes in recent years, as before, is a serious challenge for both law enforcement and legislative bodies. Every year, many people and organizations, as well as authorities, become victims of criminal offenses committed with the use of information, communication and digital technologies. Cybercrime continues to pose economic, security and technological challenges for developed and less developed countries. Society and states increasingly depend on digitization and information communications, digital technologies, which in turn increases the likelihood of cybercrime. The author suggests that criminal offenses in the field of digital technologies should be understood as a criminal, illegal, socially dangerous act provided for by the criminal law, aimed at violating the confidentiality, integrity, reliability and availability of digital information protected by law or committed with the use of digital technologies or in relation to them. The article notes that the rapid development of the field of digital technologies constantly leads not only to the appearance of new types of services in the financial sphere, but also to the improvement of methods and methods of illegally obtaining funds in the cyber environment. Significant damage is caused by criminal offenses in the digital business environment, that is, to legal entities, for whom losses from cyberattacks on finances have already become critical. It is practically impossible to assess the true scale of the negative consequences of digital crime, since not all victims are always aware and understand that they have become victims of such criminal offenses and it is impossible to accurately determine the real number of victims of, for example, phishing or hacker attacks, etc. That is why the existing legal framework for combating digital crime and other anti-criminal influence tools need to be improved. That is why the author proposes changes and additions to the criminal legislation in order to settle the researched issue.

Key words: crime, computer crime, criminal law, digitization, digital technologies, crime prevention, digital information, digital crime.

Постановка проблеми. В умовах інтенсивної цифрової інформатизації сучасного суспільства і функціонування його державних інститутів, потреба в використанні інформаційно-цифрових технологій в галузі правового регулювання є однією з найважливіших причин трансформації базових правових (і, відповідно, наукових) галузей, включаючи кримінальне право та кримінологію. У зв'язку з цим актуальним є питання щодо змісту та поняття злочинності у сфері цифрової інформації та цифрових технологій.

Загальна цифровізація, діджиталізація та інформатизація суспільства значно загострила зазначену пробле-

матику та потребує правового врегулювання. Небезпека таких кримінальних правопорушень обумовлена не лише масштабами згубних впливів, наприклад, результатами посягань на критично важливі та потенційно небезпечні інформаційні інфраструктури, а й зростанням їхньої кількості. Сьогодні з розвитком цифрових технологій значно збільшується і кількість правопорушень у сфері цифрової інформації та цифрових технологій загалом. Незважаючи на громадську небезпека подібних діянь, у теорії та практиці відсутнє єдине визначення аналізованих кримінальних правопорушень.

Незважаючи на досить часте обговорення цієї проблематики, використання інформаційно-комунікаційних та цифрових технологій у злочинних цілях в останні роки, як і раніше, є серйозним викликом як для правоохоронних, так і та законодавчих органів. Жертвами кримінальних правопорушень, вчинених з використанням інформаційно-комунікаційних та цифрових технологій, щорічно стає багато людей та організацій, а також органи влади. Кіберзлочинність продовжує створювати економічні, безпекові та технологічні проблеми для розвинутих і менш розвинених країн. Суспільство та держави все більше залежать від цифровізації та інформаційних комунікацій, цифрових технологій, що в свою чергу підвищує і ймовірність кіберзлочинності.

Вивчення та дослідження злочинності у сфері цифрових технологій є важливим з кількох причин: по-перше, цей вид злочинності стає все більш поширеною загрозою в епоху цифрових технологій і досить велика кількість користувачів мережі Інтернет стають жертвами кібератак, тому необхідно розробляти ефективніші стратегії попередження та боротьби зі злочинністю у сфері цифрових технологій; по-друге, потрібно вдосконалювати нормативно-правову базу, спрямовану на мінімізацію впливу злочинності у сфері цифрових технологій на окремих осіб, суспільство та державу загалом.

Аналіз останніх досліджень і публікацій. Кримінальну відповідальність за кіберзлочинність та кіберправопорушення загалом досліджували багато науковців, зокрема: І.І. Васильковський, О.О. Книженко, М.О. Кравцова, М.А. Погорецький, В.Б. Дзюндзюк, А.В. Савченко та інші, проте питання, що стосуються саме кримінально-правової характеристики злочинності у сфері цифрових технологій та загалом кримінальної відповідальності за правопорушення у цій сфері цілком та детально не розкриті, оскільки серед науковців є різні визначення, щодо «кіберзлочинності», «комп'ютерної злочинності», «злочинності у сфері високих технологій», «цифрової злочинності» тощо, що свідчить про актуальність та необхідність дослідження вказаної проблематики.

Постановка завдання. Метою даного дослідження є характеристика кримінальних правопорушень у сфері використання цифрових технологій та надання пропозицій щодо вдосконалення кримінально-правового законодавства у цій сфері.

Виклад основного матеріалу. Технічні інновації можна використовувати для суспільного блага, проте досить часто вони стають елементом також злочинного світу. Це більше стосується кіберзлочинності, ніж, можливо, будь-якої іншої сфери злочинності. Крім того, кіберзлочинці стають більш агресивними. Сучасні реалії такі, що цифрові технології кардинально змінили наше повсякденне життя і, водночас, створили нові види загроз безпеці інформації та всього глобального інформаційного простору. Зважаючи на те, що кіберзлочинність вчиняється у всьому світі, контекст кіберзлочинності залишається спірним, що потребує конкретизації визначення, стандартизації та класифікації кіберзлочинності.

Для визначення та класифікації кіберзлочинності використовувалися такі терміни: кіберзлочинність, комп'ютерна злочинність, електронна злочинність, інтернет-злочинність, цифрова злочинність, онлайн-злочинність, віртуальна злочинність, техно-злочинність та чиста злочинність [4, с. 8].

З розвитком цифрових технологій розвивається і кіберзлочинність, змінюються та вдосконалюються правопорушення, які вчиняються у цій сфері, так, для прикладу до них можна віднести: фішинг, несанкціонований доступ до різноманітних комп'ютерних систем і сайтів; поширення дитячої порнографії через мережу інтернет, кібергрумінг (онлайн-грумінг – це новий вид сексуального насильства дітей та підлітків в інтернеті), порушення авторських прав,

продаж нелегальних речей через мережу інтернет, різні фінансові шахрайства у віртуальному середовищі, кіберсталкінг (анонімне, приховане вистежування потерпілих задля організації злочинних дій на кшталт спроб домагання, зґвалтування, фізичного насильства, побиття. Відстежуючи через Інтернет користувачів, злочинець може отримувати інформацію про час, місце та всі необхідні умови здійснення майбутнього нападу) [1, с. 44].

Загалом, необхідно визнати, що Інтернет сьогодні набув досить значного поширення і розглядати лише комп'ютерні правопорушення не зовсім вірно, адже розвиток цифрового простору охоплює не тільки комп'ютерні технології, а й мережеві різні ресурси, інтернет-ресурси, використання гаджетів, електронно-обчислювальних машин, інформаційно-телекомунікаційних технологій тощо. Окрім цього, розвиток штучного інтелекту, блокчейну, великих даних, цифрових близнюків, хмарних програм та чат-ботів, інтегрованих в різні платформи, які також змінюють спосіб взаємодії людей з цифровим світом, свідчать про те, що цифрове життя значно розширює межі та можливості людей, а цифрове життя поступово виходить за межі комп'ютера, адже з'являється все більше і більше нових цифрових продуктів.

Подібні кримінальні правопорушення часто називають «комп'ютерними», проте кримінальні правопорушення у сфері цифрових технологій необхідно відмежовувати від кримінальних правопорушень у сфері інформаційно-телекомунікаційних технологій. Оскільки це є правопорушення, предметом яких виступає цифрова інформація і як спосіб вчинення виступають цифрові технології.

Поняття цифрової злочинності досить часто замінюють такими термінами як кіберзлочинність, електронна злочинність, комп'ютерна злочинність, тощо. Незважаючи на те, що, на відміну від інших кримінальних правопорушень, правопорушення у сфері цифрових технологій мають свої особливості. Так, вони не мають чітких географічних меж, адже можуть бути вчиненими в одній державі, а наслідки наступати абсолютно в іншій. Місцем вчинення цифрового кримінального правопорушення є віртуальне середовище; комп'ютерні дані, цифрові системи або соціальні мережі, які використовуються для його вчинення.

На сьогоднішній день суспільно небезпечні дії в галузі інформаційних правовідносин, які є загрозою громадській безпеці, особливо якщо вони пов'язані з порядком застосування комп'ютерної інформації, називаються кримінальними правопорушеннями у сфері високих технологій, тобто це сукупність злочинних діянь, вчинених за допомогою обчислювальної техніки та засобів телекомунікацій або таких, де об'єкт злочинних посягань – це комп'ютерна інформація.

Щоб посилити реагування правоохоронних органів на кіберзлочинність у ЄС і допомогти захистити європейських громадян, підприємства та уряди, Європол створив Європейський центр боротьби з кіберзлочинністю (ЕСЗ). Робота ЕСЗ зосереджена на таких напрямках: кіберзлочини, вчинені організованими групами, зокрема тими, які отримують великі кримінальні прибутки, як-от онлайн-шахрайство; кіберзлочини, які завдають серйозної шкоди жертві, наприклад, сексуальна експлуатація дітей в Інтернеті; кіберзлочини (включаючи кібератаки), що впливають на критичну інфраструктуру та інформаційні системи в Європейському Союзі. Важливою частиною цих зусиль є спеціалізація на ранньому попередженні, оцінці загроз кіберзлочинності та методах підвищення обізнаності. ЕСЗ сприяє узгодженню взаємодії правоохоронних органів у державах-членах ЄС, працюючи над колективним оглядом, який матиме важливе значення для політики, зокрема щодо визначення IP-адрес, злочинного зловживання системою доменних імен, питань акредитації конфіденційності проксі, реєстрації точних даних та потужний

механізм відповідності для акредитованих реєстраторів і реєстрів доменних імен. Досліджуючи та вдосконалюючи знання правоохоронних органів про архітектуру та структуру управління Інтернетом, ЕСЗ може отримати краще розуміння ландшафту управління Інтернетом, що стане в нагоді для розслідувань усіх держав-членів і третіх сторін [2].

Таким чином, під кримінальними правопорушеннями у сфері цифрових технологій розуміється передбачене кримінальним законом винне, протиправне, суспільно небезпечне діяння, спрямоване на порушення конфіденційності, цілісності, достовірності та доступності цифрової інформації, що охороняється законом або вчинене з використанням цифрових технологій або щодо них.

До них зокрема, можна віднести шахрайства з використанням інтернет-технологій, продаж і поширення конфіденційної інформації, шахрайські схеми в геймерській індустрії, обіг товарів та послуг, які не є легальними в правовому обігу, зростання кіберекстремізму, і особливо його найбільш небезпечної форми – кібертероризму.

Проаналізувавши кримінально-правові норми КК України, можна визначити перелік кримінальних правопорушень, які можуть вчинятися у цифровій сфері. Так, КК України містить правопорушення, які пов'язані з використанням цифрових технологій, застосуванням засобів чи способів цифрової сфери [5].

Комп'ютерна інформація, будучи елементом, що відноситься до механізму цифрової сфери, одночасно виступає ємністю, що акумулює та наповнюється змістом постійних процесів виникнення, формування, видозміни різних баз даних, інформаційних банків та інших сховищ, у яких поряд з іншими відомостями даних концентрується необхідна інформація.

Слід зазначити, що стрімкий розвиток сфери цифрових технологій постійно призводить не лише до появи нових видів послуг у фінансовій сфері, а й вдосконаленню способів та методів незаконного отримання коштів у кіберсередовищі. Значної шкоди завдають кримінальні правопорушення у цифровому середовищі бізнесу, тобто, юридичним особам, для яких вже стали критичними втрати від кібератак на фінанси. Практично неможливо оцінити справжні масштаби негативних наслідків від цифрової злочинності, оскільки не всі жертви завжди усвідомлюють та розуміють, що вони стали жертвами таких кримінальних правопорушень і неможливо точно визначити реальної кількості потерпілих від, наприклад фішингових чи хакерських атак тощо. Саме тому, існуюча правова база боротьби з цифровою злочинністю та інші антикримінальні інструменти впливу потребують вдосконалення.

Звісно ж, що кримінальні правопорушення у сфері цифрової інформації та цифрових технологій достатньо небезпечні ще й тим, що сьогодні сучасні інформаційно-телекомунікаційні технології повністю проникли у всі сфери діяльності людей і наше громадянське суспільство є повністю інформаційним та комп'ютеризованим. Через цифровий прорив виникли нові загрози інформаційній безпеці, причиною яких стала глобалізація інформаційних процесів. Відповідно, це й в свою чергу сприяє збільшенню кількості правопорушень у сфері цифрової інформації та цифрових технологій, оскільки постійно розвиваються та генеруються нові цифрові інформаційно-телекомунікаційні технології, і держава має оперативну та адекватно реагувати на подібні кримінально-протиправні діяння. Це, одноznачно, свідчить про те, що кримінально-правове законодавство про відповідальність за кримінальні правопорушення у сфері цифрової інформації та цифрових технологій потребує змін та доповнень.

Так, як бачимо, така норма, яка б передбачала кримінальну відповідальність за придбання чи збут цифрової інформації, яка одержана кримінально протиправним шляхом, відсутня. Так, інформація зазвичай не визнається

майном, і, відповідно, внаслідок маніпуляцій із нею не можна притягти особу до кримінальної відповідальності за ст. 198 КК України «Придбання, отримання, зберігання чи збут майна, одержаного кримінально протиправним шляхом». Оскільки, відповідно до ст. 190 ЦК України «Майном як особливим об'єктом вважаються окрема річ, сукупність речей, а також майнові права та обов'язки. Майнові права є неспоживною річчю. Майнові права визнаються речовими правами» [5;6].

Отже, на сьогодні цифрові технології використовуються абсолютно скрізь, адже комп'ютери, ноутбуки, планшети, смартфони, мобільні телефони тощо є атрибутами кожного суспільства. Головна мета цифрових технологій полягає в тому, щоб швидко встановити зв'язок між людьми, без зусиль і з мінімальними витратами. Люди пов'язані один з одним за допомогою величезного спектру цифрових послуг і ресурсів. Цифрова інформація дуже відрізняється від її фізичного аналогу, оскільки її можна швидко скопіювати, розподілити контрольованим чином і зберігати в різних місцях.

Потребує конкретизації і додаткового вивчення і правова природа криптовалют та необхідності захисту їх власників заходами чинного законодавства, у тому числі кримінального. Адже, швидко впроваджуються та розповсюджуються в суспільстві технологічні зміни у сфері криптовалют, яка пропонує окремі переваги перед традиційними валютами, включаючи нижчі комісії за транзакції та швидший переказ коштів за послуги. Проте, тут необхідно звернути окрему увагу на кримінологічні ризики торгівлі криптовалютою, проблему фальшивих криптовалют, фальшивих гаманців, фішингу, за допомогою якого злочинці намагаються змусити жертву надати ім'я користувача та пароль.

Американські вчені розглядають можливість застосування традиційних кримінологічних концепцій для пояснення причин злочинної діяльності у віртуальному просторі та виявлення факторів, що сприяють злочинам, пов'язаним з біткоїнами. Відповідно до закону, криптовалюта як продукт або власність визнається законодавством кількох країн. Так, податкове законодавство Австралії та законодавство США позиціонують криптовалюту як майно, яке враховується для розрахунку податку на прибуток [3].

Доцільно розмежувати поняття «електронні гроші» та «цифрові гроші». Криптовалюта може бути засобом вчинення кримінальних правопорушень. У свою чергу, криптовалюта, яка відображає предмет кримінального посягання, є цифровим активом, який має матеріальну цінність, у зв'язку з яким або з приводу якого вчинено кримінальне правопорушення.

Так, відповідно примітки до ст. 368-5 КК України «Незаконне збагачення», криптовалюта передбачена, як можливий актив, що є предметом складу кримінального правопорушення, яке передбачає кримінальну відповідальність за «набуття особою, уповноваженою на виконання функцій держави або місцевого самоврядування, активів, вартість яких більше ніж на шість тисяч п'ятсот неоподатковуваних мінімумів доходів громадян перевищує її законні доходи» [5].

Що стосується вдосконалення чинного законодавства, спрямованого на розвиток механізму протидії кримінальним правопорушенням у сфері обігу криптовалют, в першу чергу, необхідно на законодавчому рівні визначити правовий статус криптовалют, включно з її визначенням: «цифровий актив», «віртуальна валюта», «результати інтелектуальної діяльності». Окрім цього потрібно визначити права та обов'язки учасників – власників такого «товару», а також види відповідальності за протиправні посягання на цю групу суспільних правовідносин. Окрім цього, враховуючи досить значне поширення віртуальних активів на сучасному етапі, слід встановити конкретну міру кримі-

нальної відповідальності за правопорушення у сфері обігу віртуальних активів, цифрової та електронної валюти. Так, в першу чергу, доцільно визначити в межах кримінально-правової доктрини, чим виступає криптовалюта в процесі вчинення кримінального правопорушення: предметом і (або) засобом вчинення. Це важливо для його теоретичного визначення в доктрині кримінального права та правоохоронної діяльності, оскільки це поняття залежить від: визначення суб'єкта повноважень щодо протидії правопорушенням у сфері обігу даного виду активів та забезпечення координації протидії в інформаційному полі та кіберпросторі, що постійно змінюється та зростанні фактів використання криптовалют у злочинних цілях.

Висновки. Отже, цифрові можливості стають досить часто способами чи засобами вчинення кримінальних правопорушень, або ж полегшують їх вчинення. Особливість цих кримінальних правопорушень полягає в тому, що на сьогодні вони не обмежені кордонами однієї держави, вони можуть бути вчинені з будь-якого місця і проти будь-якого користувача, який знаходиться в будь-якій точці світу. На сьогодні цифрова злочинність вимагає від держав серйозних зусиль щодо боротьби з нею. Ефективність протидії їй, перш за все, залежить від міжнародної угоди про уніфікацію підходів до визначення цього негативного явища. Цифрова злочинність – це суспільне протиправне явище, яке включає сукупність кримінальних правопорушень, вчинених у сфері або з використання цифрових технологій, у тому числі нелегального отримання чи (та) поширення інформації в інформаційно-телекомунікаційних мережах, а також з використанням віртуального середовища.

Пропонуємо прирівняти цифрову інформацію до майна, адже що хоч цифрову інформацію не можна доторкнутися і відчутти, як носій інформації виступає речовий предмет (наприклад, Flash-карта), що містить цифрову інформацію та представляє матеріальну цінність. Тому, вважаємо за необхідне встановити кримінальну відповідальність за придбання або збут цифрової інформації,

яка свідомо одержана кримінально протиправним шляхом та внести зміни до КК України, шляхом доповнення його *статтею 198-1 «Придбання, отримання, зберігання чи збут цифрової інформації, одержаної кримінально протиправним шляхом» та викласти її у наступній редакції:*

«Заздалегідь не обіцяне придбання або отримання, зберігання чи збут цифрової інформації, одержаної кримінально протиправним шляхом

карається арештом на строк до шести місяців або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк».

Таким чином, незважаючи на суспільну небезпеку вказаних злочинних дій, в теорії та практиці кримінального права відсутнє єдине їх визначення, що може бути відображено як «цифрова злочинність», «кримінальні правопорушення, вчинені з використанням цифрових технологій» або «кримінальні правопорушення, вчинені у цифровій сфері». Тому, враховуючи, що на законодавчому рівні поняття «цифрова злочинність» відсутня, є необхідність внесення змін до КК України. А саме, для запобігання та протидії таким кримінальним правопорушенням, пропонуємо вдосконалити чинне кримінальне законодавство з метою чіткого правового регулювання родових та видових об'єктів кримінальних правопорушень, що вчиняються з використанням цифрових технологій, що дозволить не лише правильно кваліфікувати злочинне діяння, а й визначити правові засоби боротьби зі злочинністю у цифровій сфері та підвищити рівень цифрової безпеки і захисту громадян, суспільства та держави загалом.

Усе це дозволяє стверджувати, що поняття «цифрове кримінальне правопорушення або правопорушення у сфері цифрових технологій» є значно ширшим за поняття «кіберзлочинність» або комп'ютерна злочинність. Цифрова злочинність включає ширший спектр протиправних дій, у тому числі вчинених як з використанням комп'ютерних систем і мереж, так і з використанням цифрових технологій, у тому числі віртуального середовища, яке доповнює нашу реальність.

ЛІТЕРАТУРА

1. Batra, S., Gupta, M., Singh, J., Srivastava, D., & Aggarwal, I. (2020, November). An Empirical Study of Cybercrime and Its Preventions. In 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC). pp. 42–46.
2. European Cybercrime Centre. The Geneva Internet Platform's Digital Watch. URL: <https://dig.watch/actor/european-cybercrime-centre>
3. Kethineni S, Cao Y, & Dodge C (2018). «Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes». American Journal of Criminal Justice, 43(2), pp. 141-157.
4. McGuire, M. (2019). It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In The human factor of cybercrime (pp. 3–28).
5. Кримінальний кодекс України. Закон України від 5 квітня 2001 року. № 2341-III (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
6. Цивільний кодекс України: Закон України від 16 січня 2003 року. № 435-IV. Відомості Верховної Ради України (ВВР), 2003, №№ 40-44, ст.356. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>