DOI DOI: https://doi.org/10.32353/acfs.12.2025.05
УДК 343.985 (477)

Анастасія Вуйма

Анастасія Вуйма
докторка філософії за спеціальністю 081 «Право»,
доцентка кафедри криміналістики та судової експертології навчально-наукового інституту № 1 Харківського національного університету внутрішніх справ,
м. Харків, Україна;
ORCID: http://orcid.org/0000-0002-6215-5361
e-mail: avuima@ukr.net

Цифровий вимір сучасної злочинності: кіберпростір як типова обстановка вчинення кримінальних правопорушень

У статті розглянуто проблему визначення кіберпростору як обстановки вчинення кримінального правопорушення, розкрито іманентні ознаки цієї категорії. Здійснено критичний аналіз традиційних криміналістичних підходів до структури обстановки злочину, які базуються на матеріально-фізичному розумінні середовища. Обґрунтовано неможливість застосування цих підходів до злочинів, що вчиняються у цифровому середовищі, та визначено специфіч-ні ознаки кіберпростору як криміналістично значущої реальності. Представлено криміналістичну класифікацію кримінальних право-порушень, що можуть бути скоєні у кіберпросторі, з урахуванням мотиваційного чинника та об'єктно-функціональної спрямованос-ті. Запропоновано адаптовану криміналістичну класифікацію обстановки кіберзлочинів за стадією реалізації діяння, динамікою змін її елементів, впливом на кримінальну поведінку та ступенем прогно-зованості. Наголошено на необхідності формування нових методич-них підходів до дослідження цифрової обстановки задля підвищення ефективності досудового розслідування в умовах цифровізації.

Ключові слова: *злочинність, кримінальне правопорушення, криміналістична методика, криміналістична характеристика, обстановка вчинення злочину, цифрове середовище, кіберпростір, цифровий слід.*

Постановка наукової проблеми. У XXI ст. стрімкий розвиток інформаційно-комунікаційних технологій продовжив докорінно трансформувати суспільні відносини, включаючи механізми вчинення кримінальних правопорушень. Кіберпростір, що охоплює глобальні цифрові мережі, електронні комунікації та інформаційні ресурси, перетворився на нове, складне та багатоаспектне середовище для злочинної діяльності. У сучасних умовах злочини в кіберпросторі набули не лише кількісного поширення, а й якісної трансформації: кіберпростір перестає бути лише інструментом злочину, натомість стає повноцінною обстановкою, у межах якої відбувається підготовка, безпосередньо реалізується та приховуються слідичи окремі наслідки протиправної діяльності.

Попри це, криміналістика ще не виробила комплексного підходу до визначення правової природи кіберпростору як обстановки вчинення кримінального правопорушення. Існуючі концепти, що стосуються місця, способу, часу та умов учинення злочину, потребують актуалізації з урахуванням специфіки цифрового середовища. Окрім того, залишається відкритим питання щодо визначення сутності поняття «обстановка вчинення злочину» в контексті віртуальної діяльності, а також способів її дослідження, особливостей наукового осмислення, фіксації та аналізу під час досудового розслідування.

Таким чином, постає наукова потреба в уточненні теоретичних підходів до розуміння кіберпростору як складової обстановки вчинення кримінального правопорушення, а також у розробленні методичних засад його

ФІНАНСУВАННЯ

Це дослідження не отримувало жодних спеціальних грантів від фінансуючих організацій у державному, комерційному чи некомерційному секторах.

ЗАСТЕРЕЖЕННЯ

Фінансуюча сторона не брала участі в розробці дизайну дослідження, зборі та аналізі даних, прийнятті рішення про публікацію або підготовці рукопису.

УЧАСНИКИ

Автор брав участь виключно в інтелектуальній дискусії, що лежить в основі цієї статті, дослідженні прецедентного права, написанні та редагуванні, і несе відповідальність за зміст та інтерпретацію.

ДЕКЛАРАЦІЯ ПРО КОНФЛІКТ ІНТЕРЕСІВ

Автор заявляє, що у нього немає конфлікту інтересів.

дослідження для потреб криміналістики, кримінального процесу, оперативно-розшукової діяльності, кібербезпеки тощо.

Аналіз основних досліджень і публікацій. Вагомий внесок у розвиток криміналістичної науки в частині методики розслідування злочинів, учинених у кіберпросторі зробила О. Самойленко. У своїй монографії авторка вперше комплексно розглянула кіберпростір як особливу обстановку вчинення злочину, що зумовлює специфіку формування криміналістичної характеристики. Вона акцентувала увагу на необхідності врахування цифрової природи слідів, динаміки цифрового середовища та його впливу на всі стадії розслідування [1]. Подібні питання досліджували також А. Бенескул [2], Ю. Виходець зі співавторами [3], Р. Нестеренко [4], А. Рейнгольд [5] та інші. Їхні праці утворюють теоретичну основу для формування оновлених криміналістичних підходів, адаптованих до умов функціонування цифрового суспільства.

Мета статті – з'ясувати криміналістичні особливості обстановки вчинення кримінальних правопорушень у цифровому середовищі.

Викладення основного матеріалу дослідження. У криміналістичній характеристиці злочинів обстановка є системним відображенням зовнішніх умов, у яких реалізується злочинний умисел. У науковій літературі вказують, що структура обстановки охоплює три взаємопов'язані компоненти: матеріальне середовище (об'єкти та явища, що становлять фізичний простір злочину), мікросоціальне (найближче соціальне оточення, у тому числі міжособистісні зв'язки) та морально-психологічне (панівні настрої, переконання, психоемоційні стани учасників події) [6].

Висвітлюються й інші позиції щодо розуміння сутності поняття обстановки. Зокрема, Д. Четвертак пропонує визначати обстановку як сукупність фізично-матеріальних і соціальних умов, що або свідомо обрані злочинцем, або об'єктивно його оточують, у межах яких реалізується кримінальне діяння, і які впливають на формування всіх складових злочину та визначають напрями й засоби його розслідування [7]. Своєю чергою обстановку приховування злочинів автор пропонує розуміти як сукупність фізично-матеріальних і соціальних умов, у яких особа реалізує дії, спрямовані на ускладнення викриття злочину. Ця система включає місце, час, погодні умови, предметне оточення (знаряддя та засоби), соціальний статус і матеріальне становище виконавця, його особисті стосунки з особою, що вчинила первинне правопорушення, а також психологічний стан усіх учасників. Усі ці чинники взаємодіють між собою, впливаючи на характер злочинного задуму та визначаючи напрями його розслідування [8].

На сьогодні у криміналістиці досі відсутній уніфікований підхід як до визначення самого поняття «обстановка вчинення кримінального правопорушення», так і до розуміння його структурних складових. Л. Курята та А. Мировська, які вивчали цю проблему узагальнюючи існуючі наукові підходи до трактування цього феномена. Так, перша група науковців розглядають обстановку як конкретні та специфічні об'єктивні умови,

[1] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

[2] Бенескул А. В. Характеристика кримінальних правопорушень у сфері використання цифрових технологій. *Юридичний науковий електронний журнал*. 2021. № 12. С. 511-514. DOI: https://doi.org/10.32782/2524-0374/2021-12/131.

[3] Теоретичні та праксеологічні засади розслідування кримінальних правопорушень у кіберпросторі : монографія / Ю. О. Виходець, В. Г. Дрозд, М. М. Єфімов, В. Б. Коба, І. О. Луговий та ін.; МВС України, ДЗДГ Національної поліції України, Дніпр. держ. ун-т внутр. справ. Дніпро: ДДУВС, 2025. 212 с.

[4] Ващенко І. О. Кіберпростір як обстановка вчинення злочинів у сфері наркобізнесу. *Порівняльно-аналітичне право*. 2019. № 2. С.226-228.

[5] Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції: автореф. дис. … канд. юрид. наук : 12.00.09. Дніпро, 2023. 25 с.

[6] Динту В. А. Обстановка злочину як елемент криміналістичної характеристики злочинів: автореф. дис. ... канд. юрид. наук : 12.00.09. Одеса, 2014. С. 13.

[7] Четвертак Д. Ю. Характеристика обстановки вчинення приховування злочинів. *Національний юридичний журнал: теорія та практика*. 2015. № 3. С. 85–88.

[8] Четвертак Д. Ю. Методика розслідування приховування злочинів : дис. … канд. юрид. наук: 12.00.09. Харків, 2016. 218 с.

Анастасія Вуйма

ЦИФРОВИЙ ВИМІР СУЧАСНОЇ ЗЛОЧИННОСТІ: КІБЕРПРОСТІР ЯК ТИПОВА ОБСТАНОВКА ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

У статті розглянуто проблему визначення кіберпростору як обстановки вчинення кримінального правопорушення, розкрито іманентні ознаки цієї категорії. Здійснено критичний аналіз традиційних криміналістичних підходів до структури обстановки злочину, які базуються на матеріально-фізичному розумінні середовища. Обґрунтовано неможливість застосування цих підходів до злочинів, що вчиняються у цифровому середовищі, та визначено специфічні ознаки кіберпростору як криміналістично значущої реальності. Представлено криміналістичну класифікацію кримінальних правопорушень, що можуть бути скоєні у кіберпросторі, з урахуванням мотиваційного чинника та об'єктно-функціональної спрямованості. Запропоновано адаптовану криміналістичну класифікацію обстановки кіберзлочинів за стадією реалізації діяння, динамікою змін її елементів, впливом на кримінальну поведінку та ступенем прогнозованості. Наголошено на необхідності формування нових методичних підходів до дослідження цифрової обстановки задля підвищення ефективності досудового розслідування в умовах цифровізації.

Ключові слова: злочинність, кримінальне правопорушення, криміналістична методика, криміналістична характеристика, обстановка вчинення злочину, цифрове середовище, кіберпростір, цифровий слід.

Anastasiia Vuima

DIE DIGITALE DIMENSION DER MODERNEN KRIMINALITÄT: DER CYBERRAUM ALS TYPISCHE TATUMGEBUNG BEI STRAFTATEN

Zusammenfassung. Der Artikel betrachtet das Problem der Definition des Cyberraums als Tatumgebung einer Straftat und legt die immanenten Merkmale dieser Kategorie dar. Es erfolgt eine kritische Analyse traditioneller kriminalistischer Ansätze zur Struktur der Tatumgebung, die auf einem materiell-physischen Verständnis der Umwelt basieren.

Begründet wird die Unmöglichkeit der Anwendung dieser Ansätze auf Verbrechen, die im digitalen Umfeld begangen werden, und es werden die spezifischen Merkmale des Cyberraums als kriminalistisch signifikante Realität bestimmt. Vorgestellt wird eine kriminalistische Klassifikation von Straftaten, die im Cyberraum begangen werden können, unter Berücksichtigung des motivationalen Faktors und der objekt-funktionalen Ausrichtung. Vorgeschlagen wird eine adaptierte kriminalistische Klassifikation der Umgebung von Cyberverbrechen nach dem Stadium der Tatrealisierung, der Dynamik der Veränderung ihrer Elemente, dem Einfluss auf das kriminelle Verhalten und dem Grad der Vorhersehbarkeit. Betont wird die Notwendigkeit der Entwicklung neuer methodischer Ansätze zur Untersuchung der digitalen Umgebung zwecks Steigerung der Effizienz des Vorverfahrens unter den Bedingungen der Digitalisierung.

Schlüsselwörter: Kriminalität, Straftat, kriminalistische Methodik, kriminalistische Charakteristik, Tatumgebung, digitales Umfeld, Cyberraum, digitaler Fußabdruck.

Anastasiia Vuima

LA DIMENSION NUMÉRIQUE DE LA CRIMINALITÉ MODERNE : LE CYBERESPACE EN TANT QU'ENVIRONNEMENT TYPIQUE POUR COMMETTRE DES INFRACTIONS PÉNALES

L'article examine le problème de la définition du cyberespace comme lieu de commission d'une infraction pénale et révèle les caractéristiques immanentes de cette catégorie. Une analyse critique des approches criminologiques traditionnelles de la structure du lieu du crime, basées sur une compréhension matérielle et physique de l'environnement, a été réalisée. L'impossibilité d'appliquer ces approches aux crimes commis dans l'environnement numérique est justifiée et les caractéristiques spécifiques du cyberespace en tant que réalité criminalistique significative sont définies. Une classification criminalistique des infractions pénales pouvant être commises dans le cyberespace est présentée, en tenant compte du facteur motivationnel et de l'orientation objective et fonctionnelle. Une classification criminalistique adaptée des cybercrimes est proposée en

у яких реалізується суспільно небезпечне посягання. Друга група дослідників трактує обстановку як сукупність подій і обставин, що характеризують суспільну небезпечність діяння та створюють умови для досягнення злочинцем своєї мети. Третя група науковців визначає обстановку як комплекс матеріальних і соціально-психологічних елементів середовища, яке безпосередньо оточує особу злочинця, є результатом свідомого вибору ним місця і умов для вчинення злочину, здатне впливати на формування інших елементів криміналістичної характеристики та зумовлювати методику розслідування [9].

Така багатоманітність, попри все, не враховує сучасної трансформації середовища вчинення злочинів, що зумовлені цифровізацією суспільних процесів. Зокрема, у них не враховується можливість реалізації злочинного умислу у кіберпросторі, який дедалі частіше стає самостійною або додатковою складовою обстановки вчинення кримінального правопорушення. Цифрове середовище, сформоване внаслідок функціонування об'єднаних комунікаційних систем і платформ, створює нову реальність, у межах якої здійснюються суспільно небезпечні посягання – від шахрайства до злочинів проти основ національної безпеки. Відтак, ігнорування цієї складової у структурі обстановки злочину не лише звужує її понятійний зміст, а й ускладнює процес розслідування, унеможливлюючи повне встановлення обставин кримінального правопорушення. Таким чином, виникає необхідність широкого підходу до тлумачення обстановки злочину, що передбачає включення до її структури й кіберпросторової компоненти як рівнозначного елементу поряд із матеріальним, мікросоціальним і морально-психологічним середовищем.

Аргументування підходу щодо віднесення віртуального (цифрового) середовища або кіберпростору як типової обстановки вчинення злочину у XXI столітті, вимагає розкриття дефініцій цих категорій. На нормативному рівні, зокрема в Законі України «Про основні засади забезпечення кібербезпеки України» визначено, що кіберпростір – це віртуальне середовище, що виникає внаслідок функціонування взаємопов'язаних комунікаційних систем і забезпечує можливість електронної взаємодії та реалізації суспільних відносин за допомогою Інтернету або інших глобальних мереж передачі даних.

У сучасному правовому дискурсі широкого поширення набув термін «віртуальний простір», який здебільшого вживається як синонім поняття «кіберпростір». Під ним розуміють змодельоване за допомогою комп'ютерних технологій інформаційне середовище, у межах якого функціонують цифрові відображення осіб, предметів, фактів, подій, явищ і процесів. Ці відображення можуть бути представлені в математичній, символьній або іншій формі та перебувати в динамічному обігу в локальних або глобальних комп'ютерних мережах. Крім того, йдеться також про дані, які зберігаються на фізичних або віртуальних пристроях, чи інших носіях, призначених для накопичення, оброблення й передавання інформації [10].

Узагальнюючи викладене, можна стверджувати, що сучасне розуміння обстановки вчинення кримінального правопорушення потребує суттєвого оновлення з урахуванням трансформації суспільних відносин під впливом цифровізації. Кіберпростір і віртуальний простір (цифрове середовище), сформовані внаслідок функціонування об'єднаних інформаційно-комунікаційних систем, набули ознак самостійної криміналістично значущої реальності. Вони стали не лише засобом, а й самостійною обстановкою вчинення злочину, в межах якої відбувається формування, реалізація та приховування злочинного умислу. Врахування кіберпростору як повноцінного елементу структури обстановки злочину є необхідною передумовою для адекватного вивчення та документування злочинної діяльності в умовах цифрового суспільства та ефективного її розслідування. Такий підхід відкриває перспективи для формування

[9] Курята Л., Мировська А. Обстановка шахрайства, вчиненого під приводом проповідування віровчень і виконання релігійних обрядів, та її значення для розслідування. *Підприємництво, господарство і право*. 2021. № 5. С. 259. DOI https://doi.org/10.32849/2663-5313/2021.5.42.

[10] Кіпа О. Правопорушення в мережі Інтернет. *Часопис Київського університету права.* 2010. № 4. С. 346-349.

нових методичних засад у криміналістиці, орієнтованих на цифрову реальність.

На шляху пізнання сутності будь-якого явища, не можна оминути увагою іманентні ознаки кіберпростору. У контексті обстановки вчинення злочину вчені виходять з можливості аналізування її як на теоретичному рівні – через систему типових умов, що формують контекст злочину, – так і на прикладному, де вона постає як предмет слідчого аналізу, що підлягає всебічному вивченню, документуванню та інтерпретації задля забезпечення ефективного розслідування.

Досить повно визначає обстановку вчинення кримінального правопорушення з позицій криміналістики В. Тіщенко, який розглядає її як систему, що включає такі елементи:

– хронологічні характеристики розвитку злочинної події;
– просторові параметри на всіх етапах її перебігу;
– матеріальне оточення місць підготовки, реалізації та приховування злочину;
– погодні й інші природно-кліматичні умови;
– поведінкові реакції учасників кримінальної події;
– соціально-побутові та психологічні взаємини;
– загальні умови, на тлі яких розгорталася подія злочину;
– чинники, що сприяли або перешкоджали підготовці, вчиненню й приховуванню злочину [11].

Попри грунтовність наведеного підходу, позиція В. Тіщенка не може вважатися універсальною в контексті криміналістичної характеристики злочинів, що вчиняються у кіберпросторі. Його підхід, сформований на основі традиційного розуміння матеріальної, часової, просторової, природно-кліматичної та соціально-психологічної обстановки, значною мірою орієнтований на злочини, що реалізуються у фізичному (офлайн) середовищі. Водночас більшість характеристик, наведених автором, втрачають свою релевантність або вимагають суттєвої трансформації в разі розуміння цього питання крізь призму цифрового середовища.

Кримінальні правопорушення, вчинені у кіберпросторі мають іншу природу. Їх обстановка не може бути охарактеризована через фізичні межі простору чи погодні умови, оскільки віртуальне середовище не обмежене географією та часом у традиційному розумінні. Наприклад, фішинг чи шахрайство з використанням платіжних систем, відмивання грошових коштів або розповсюдження порнографічних предметів можуть бути вчинені одночасно в кількох країнах, без безпосереднього фізичного контакту або визначеного місця вчинення. Поведінка суб'єктів злочину, співучасників також має іншу форму – вона фіксується не через безпосереднє спостереження, а через цифрові сліди: лог-файли, IP-адреси, дії в мережі, активність у віртуальному середовищі.

Вважаємо, що обстановка вчинення кіберзлочину (учинених у кіберпросторі) характеризується такими ознаками:

– нематеріальність простору – відсутність конкретного фізичного місця, натомість – віртуальні локації: сервери, облікові записи, платформи;
– інформаційна основа – злочин вчиняється шляхом оперування даними, кодами, цифровими активами;
– технологічна посередкованість – реалізація діяння через інструменти інформаційно-комунікаційних технологій, із використанням програмного забезпечення, через мережеву інфраструктуру;
– асинхронність – події можуть відбуватися неодночасно, розтягнуто в часі, що ускладнює визначення хронології;
– неоднозначність групи залучених суб'єктів – злочинець може діяти анонімно або під іменем третьої особи, а учасники події можуть навіть не усвідомлювати своєї «залученості» до злочинної діяльності;
– відсутність фізичних слідів – докази мають цифрову природу (електронні журнали, метадані, знімки екранів, цифрові підписи).

Тобто, традиційна структура обстановки злочину, орієнтована на фізичне середовище, потребує перегляду й адаптації, щоб охопити особливості кіберпростору.

[11] Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. С. 69.

fonction du stade de réalisation de l'acte, de la dynamique des changements de ses éléments, de son influence sur le comportement criminel et de son degré de prévisibilité. La nécessité de développer de nouvelles approches méthodologiques pour l'étude de l'environnement numérique afin d'améliorer l'efficacité des enquêtes préliminaires dans le contexte de la numérisation est fait remarquer.

Mots-clés : crime, infraction pénale, méthodologie criminalistique, caractérisation criminalistique, scène de crime, environnement numérique, cyberespace, empreinte numérique.

Anastasiia Vuima

CYFROWY WYMIAR WSPÓŁCZESNEJ PRZESTĘPCZOŚCI: CYBERPRZESTRZEŃ JAKO TYPOWA SYTUACJA POPEŁNIANIA PRZESTĘPSTW

W artykule omówiono problem definiowania cyberprzestrzeni jako miejsca popełnienia przestępstwa kryminalnego oraz ujawniono immanentne cechy tej kategorii. Przeprowadzono krytyczną analizę tradycyjnych kryminalistycznych podejść do struktury miejsca przestępstwa, opartych na materialno-fizycznym rozumieniu środowiska. Uzasadniono niemożność zastosowania tych podejść do przestępstw popełnianych w środowisku cyfrowym oraz określono specyficzne cechy cyberprzestrzeni jako rzeczywistości istotnej z kryminalistycznego punktu widzenia. Przedstawiono kryminalistyczną klasyfikację przestępstw kryminalnych, które mogą być popełnione w cyberprzestrzeni, z uwzględnieniem czynnika motywacyjnego i obiektowo-funkcjonalnego ukierunkowania. Zaproponowano dostosowaną klasyfikację kryminalistyczną sytuacji cyberprzestępstw według etapu realizacji czynu, dynamiki zmian jego elementów, wpływu na zachowania przestępcze i stopnia przewidywalności. Podkreślono konieczność kształtowania nowych metodologicznych podejść do badania sytuacji cyfrowej w celu zwiększenia skuteczności dochodzenia przedprocesowego w warunkach cyfryzacji.

Słowa kluczowe: przestępczość, przestępstwo kryminalne, metodyka kryminalistyczna, charakterystyka kryminalistyczna, sytuacja popełnienia przestępstwa, środowisko cyfrowe, cyberprzestrzeń, ślad cyfrowy.

бливості кіберпростору як специфічної обстановки вчинення кримінальних правопорушень у XXI столітті.

Для цілей криміналістичної класифікації злочинів, учинених у кіберпросторі, як слушно визначила О. Самойленко, доцільно виходити із традиційних сфер суспільного життя, які визначають мотиви протиправної діяльності суб'єктів цифрового середовища. У такому контексті мотивація стає системоутворюючим чинником, що впливає на вибір об'єкта посягання, характер кримінальних дій і спосіб реалізації злочинної мети. З огляду на це пропонується виділяти такі основні групи мотивів:

1. Корисливі мотиви, пов'язані з фінансово-економічними відносинами суб'єктів у кіберпросторі.
2. Соціально-економічні мотиви, що зумовлені потребами чи очікуваннями, пов'язаними з соціальною сферою цифрової взаємодії.
3. Антидержавно-політичні мотиви, що виникають у контексті державнополітичних відносин у цифровому середовищі.
4. Ідейні мотиви, які обумовлені світоглядними та ціннісно-світоглядними орієнтаціями суб'єктів у кіберпросторі.

На підставі такої мотиваційної класифікації вчена структурує і самі кримінальні правопорушення, вчинені в кіберпросторі, у відповідні групи, серед яких:

1. Злочини з корисливих мотивів, що мають економічний характер і спрямовані на отримання неправомірної вигоди.
2. Злочини з соціально-економічних мотивів, які пов'язані з порушенням соціальних норм і мають негативні наслідки для окремих соціальних груп або інформаційного середовища.
3. Злочини з антидержавно-політичних мотивів, що мають на меті дестабілізацію державних інститутів або порушення політичної безпеки.
4. Злочини з ідейних мотивів, які випливають із системи світоглядних цінностей виконавця та відображаються у контентно-орієнтованих діях у цифровому середовищі.

На основі аналізу судово-слідчої практики запропоновано таку класифікацію злочинів у кіберпросторі:

1. Злочини з корисливих мотивів, пов'язані з фінансово-економічною сферою (підгрупи):
1.1. Порушення режиму обігу предметів обмеженого доступу.
1.2. Протиправні дії, спрямовані на заволодіння майном (зокрема шляхом електронних розрахунків).
1.3. Порушення господарської діяльності, пов'язані з монополізмом чи недобросовісною конкуренцією.
2. Злочини з соціально-економічних мотивів, що включають насильницько-егоїстичні дії та порушення комунікаційних прав (підгрупи):
2.1. Дії, що спричиняють шкоду фізичному чи психологічному стану осіб.
2.2. Порушення прав інтелектуальної власності та таємниці комунікацій.
3. Злочини з антидержавно-політичних мотивів, пов'язані із загрозою національній безпеці та політичними інтересами держави (підгрупи):
3.1. Антидержавницькі дії, спрямовані на підірвання конституційного порядку.
3.2. Порушення у сфері державної таємниці.
3.3. Протиправні втручання в автоматизовані системи державних інститутів.
3.4. Політико-ідеологічні злочини, зокрема терористичні акти та порушення виборчих прав.
4. Злочини з ідейних мотивів, які випливають із дискримінаційних або радикальних світоглядних установок (підгрупи):
4.1. Насильницько-дискримінаційні дії.
4.2. Анархістські дії, пов'язані з використанням електронно-обчислювальних систем [12].

З урахуванням наведеної класифікації, актуальних тенденцій у правозастосовній практиці, визначених вище характеристик обстановки кіберзлочинів і специфіки цифрового середовища, можемо запропонувати удосконалену криміналістичну класифікацію кримінальних правопорушень, учинених у кіберпросторі, що враховує як мотиваційний чинник, так і об'єктно-спрямовану спрямованість дій особи злочинця. Вважаємо, що до неї слід відносити такі групи кримінально-караних діянь:

1. Кримінальні правопорушення, учинені з корисливих мотивів, тобто які: спрямовані на привласнення або перерозподіл цифрових, фінансових чи матеріальних активів, у тому числі криптовалюти. Вони охоплюють такі діяння:
1.1. Фінансово-маніпулятивні злочини: шахрайство, фішинг, відмивання грошей, крадіжки грошових активів з банківських платіжних карток та електронних гаманців тощо.
1.2. Технологічне піратство: незаконне використання ліцензій, порушення систем захисту цифрових продуктів.
1.3. Цифрове рейдерство та недобросовісна конкуренція: протидія законній господарській діяльності, розголошення комерційної таємниці тощо.
2. Кримінальні правопорушення, скоєні з мотивів ревнощів, помсти тощо (контроль, вплив, задоволення потреб), зокрема, пов'язані з експлуатацією осіб, маніпулятивною поведінкою, особистою вигодою тощо. До цієї групи можна віднести

[12] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. С. 63-66.

2.1. Окремі кримінальні правопорушення проти волі, честі та гідності: вербування з метою торгівлі людьми, кібербулінг (насильство в цифровому середовищі), доведення до самогубства тощо.

2.2. Розповсюдження порнографічних предметів: виготовлення, зберігання, розповсюдження порнографії, зокрема дитячої.

2.3. Посягання на інтелектуальну сферу: порушення авторського права, порушення права на приватність, викрадення або розголошення персональних даних.

3. Кримінальні правопорушення, реалізовані з антидержавних і політичних мотивів, тобто які мають за мету підрив державних інституцій, дестабілізацію політичного ладу, втручання в державні процеси. До цієї групи можна віднести:

3.1. Кібератаки проти державної інфраструктури: втручання в інформаційні системи органів влади, у тому числі органи правосуддя, саботаж виборчих процесів.

3.2. Порушення у сфері держтаємниці та шпигунство: кіберрозвідка, незаконний доступ до баз даних та відомостей, що становлять охоронювану законом таємницю.

3.3. Цифрова пропаганда та глорифікація війни: розповсюдження закликів до насильницької зміни влади, воєнної агресії, тероризму.

4. Кримінальні правопорушенняз ідейних та світоглядно-екстремістських мотивів, тобто вчинені з релігійної, расової, націоналістичної або анархістської позицій, часто спрямовані на підрив суспільних цінностей, а саме:

4.1. Мовно-релігійна або расова дискримінація: пропаганда ненависті, розпалювання ворожнечі, цькування.

4.2. Кібер-анархізм та деструктивний хактивізм: атаки на цифрові інфраструктури заради демонстрації протесту, ідеологічного маніфесту.

4.3. Кримінальні правопорушення проти інформаційної безпеки, порушення інформаційних систем або протиправних дій із даними,

Слід звернути увагу на те, що класифікація обстановки можлива за кількома критеріями: залежно від стадії злочинної діяльності (підготовка, реалізація, приховування), характеру змін її елементів (статична чи динамічна), впливу на кримінальну поведінку (сприятлива або несприятлива) та ступеня прогнозованості (передбачувана або непередбачувана) [13]. Разом із цим, кіберпростір набуває особливих рис як обстановка вчинення кримінального правопорушення.

На відміну від традиційного фізичного середовища, цифрове середовище може охоплювати всі етапи злочинної діяльності – від підготовки до реалізації та приховування. При цьому, підготовка до злочину у кіберпросторі здійснюється через використання спеціалізованих програмних засобів, платформ та інфраструктури, що унеможливлює прив'язку до конкретної території чи часового проміжку. Реалізація злочинного умислу, як правило, є віддаленою, опосередкованою і подекуди автоматизованою. Приховування злочину також має особливий характер: воно базується на методах цифрової анонімізації (наприклад, шляхом підключення до мережі через VPN), шифрування чи кодування інформації, використання розподілених обчислювальних мереж, що ускладнює виявлення причетних осіб та фіксацію цифрових слідів.

За характером змін своїх елементів кіберпростір постає як динамічне, змінне середовище, у межах якого цифрові об'єкти можуть бути оперативно створені, змінені або знищені. Це позбавляє можливості фіксації стабільної, статичної обстановки злочину, що характерна для традиційних форм кримінально-караної поведінки. Натомість, виявлення й аналіз такої обстановки вимагає оперативного технічного втручання та візуалізації складних зв'язків у цифровому середовищі.

Щодо впливу обстановки на кримінальнь-карану поведінку, то кіберпрострі забезпечує знеособлення, анонімність, доступність цільової аудиторії та інструментів вчинення злочину, що суттєво знижує ризики викриття всіх осіб, причетних до вчинення кримінального правопорушення. Проте одночасно цифрове середовище залишає специфічні сліди (цифрові сліди, лог-файли, метадані), що за умови належного технічного супроводу, можуть бути виявлені, зафіксовані та досліджені у кримінальному провадженні.

У розрізі критерію прогнозованості обстановка злочину скоріше є непередбачуваною. Цифрові інструменти дозволяють швидко адаптувати злочинні схеми до сформованої цифрової реальності, змінювати способи реалізації злочинного умислу, змінювати об'єкти посягання. Це створює додаткові складнощі для органів досудового розслідування, які змушені постійно вдосконалювати свої аналітичні й технічні спроможності, орієнтуючись не на традиційні, а на інтерактивні та змінні параметри цифрового середовища. Таким чином, обстановка кіберпростору є відносно новою криміналістичною категорією, що потребує переосмислення усталених підходів до її розуміння, тлумачення, дослідження й фіксації.

Висновки. Традиційні уявлення про обстановку вчинення кримінального правопорушення, сформовані в межах класичної криміналістичної доктрини, виявляються недостатніми для адекватного відображення специфіки злочинної діяльності в умовах кіберпростору. Цифрове середовище, яке дедалі частіше є не лише інструментом, а й повноцінною обстановкою вчинення кримінального правопорушення, має низку унікальних характеристик, зокрема нематеріальність, інформаційно-комунікаційну природу, технологічну опосередкованість, асинхронність, анонімність учасників і циф-

[13] Динту В. А. Обстановка злочину як елемент криміналістичної характеристики злочинів : автореф. дис. ... канд. юрид. наук : 12.00.09. Одеса, 2014. С. 13-15.

ровий характер слідів. Це обумовлює потребу в системному оновленні теоретичних засад криміналістики, зокрема перегляді концепції обстановки злочину з урахуванням трансформаційних процесів, пов'язаних із цифровізацією. Кіберпростір охоплює всі стадії злочинної діяльності, від підготовки до реалізації та приховування, а його динамічність, висока варіативність і складність фіксації слідів висувають нові вимоги до формування методико-криміналістичних рекомендацій щодо розслідування окремих кримінальних правопорушень.

Запропонована класифікація кіберзлочинів з урахуванням мотиваційних і об'єктно-функціональних критеріїв є лише спробою на шляху осмислення актуального питання. Наявність таких типів мотивів, як корисливі, соціально-економічні, антидержавно-політичні й ідейні, вказує на багатовекторність цифрової злочинності, що нині охопила майже всі сфери суспільного життя.

Таким чином, кіберпростір як обстановка вчинення злочину потребує інституціоналізації у криміналістиці, розробки адаптованих методичних підходів до його аналізу, фіксації та дослідження, а також формування нової парадигми криміналістичного мислення, зорієнтованої на виклики цифрової епохи.

References

Beneskul, A. V. (2021). Kharakterystyka kryminalnykh pravoporushen u sferi vykorystannia tsyfrovykh tekhnolohii. *Yurydychnyi naukovyi elektronnyi zhurnal*, 12, 511–514. https://doi.org/10.32782/2524-0374/2021-12/131 [in Ukrainian].

Vashchenko, I. O. (2019). Kiberprostir yak obstanovka vchynennia zlochyniv u sferi narkobiznesu. *Porivnialno-analitychne pravo*, 2, 226–228 [in Ukrainian].

Dyntu, V. A. (2014). Obstanovka zlochynu yak element kryminalistychnoi kharakterystyky zlochyniv: avtoref. dys. ... kand. yuryd. nauk: 12.00.09. Odesa. 20 s [in Ukrainian].

Kipa, O. (2010). Pravoporushennia v merezhi Internet. *Chasopys Kyivskoho universytetu prava*, 4, 346–349 [in Ukrainian].

Kuriata, L., & Myrovska, A. (2021). Obstanovka shakhraistva, vchynenoho pid pryvodom propoviduvannia virovchen i vykonannia relihiinykh obriadiv, ta yii znachennia dlia rozsliduvannia. *Pidpryiemnytstvo, hospodarstvo i pravo*, 5, 258–262. https://doi.org/10.32849/2663-5313/2021.5.42 [in Ukrainian].

Reinhold, A. V. (2023). Osnovy metodyky rozsliduvannia shakhraistva v internet-komertsii: avtoref. dys. … kand. yuryd. nauk: 12.00.09. Dnipro. 25 s [in Ukrainian].

Samoilenko, O. A. (2020). Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori : monohrafiia / za zah. red. A. F. Volobuieva. Odesa: TES. 372 s [in Ukrainian].

Vykhodets, Yu. O., Drozd, V. H., Yefimov, M. M., Koba, V. B., Luhovyi, I. O., ta in. (2025). Teoretychni ta prakseolohichni zasady rozsliduvannia kryminalnykh pravoporushen u kiberprostori : monohrafiia. Dnipro: Dnipr. derzh. un-t vnutr. sprav. 212 s [in Ukrainian].

Tishchenko, V. V. (2007). Teoretychni i praktychni osnovy metodyky rozsliduvannia zlochyniv : monohrafiia. Odesa: Feniks. 260 s [in Ukrainian].

Chetvertak, D. Yu. (2016). Metodyka rozsliduvannia prykhovuvannia zlochyniv: dys. … kand. yuryd. nauk: 12.00.09. Kharkiv. 218 s [in Ukrainian].

Chetvertak, D. Yu. (2015). Kharakterystyka obstanovky vchynennia prykhovuvannia zlochyniv. *Natsionalnyi yurydychnyi zhurnal: teoriia ta praktyka*, 3, 85–88 [in Ukrainian].

Надійшла до редколегії: 14.07.2025 / Рецензовано 12.08.2025 / Прийнято до друку 17.10.2025 / Доступно онлайн 30.01.2026

Приклад цитування:

Вуйма, А. (2025). Цифровий вимір сучасної злочинності: кіберпростір як типова обстановка вчинення кримінальних правопорушень *Архів кримінології та судових наук*. 2 (12). 64-70. DOI: https://doi.org/10.32353/acfs.12.2025.05