DOI: 10.33663/0869-2491-2026-37-882-892
УДК 340.1

К. К. ТЕТРУЄВ
*аспірант Інституту держави і права імені В. М. Корецького**
ORCID: 0009-0009-8872-8966

ПРОТИПРАВНА ПОВЕДІНКА У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ПІДХОДИ ДО РОЗУМІННЯ

У статті здійснено теоретико-правовий аналіз протиправної поведінки у сфері інформаційних технологій як складного багатофазного та гібридного правового феномена, що формується в умовах цифровізації суспільних відносин. Обґрунтовано обмеженість традиційних кримінально-правових підходів до кваліфікації цифрових діянь, які не враховують їх процесуальну динаміку, алгоритмічну опосередкованість і маскувальні механізми. Запропоновано концептуальну модель структури кіберправопорушення, що відображає послідовність його фаз та дає змогу уточнити межі суб'єктності, об'єктивної сторони й ступінь суспільної небезпеки. Практичне значення дослідження полягає у можливості використання отриманих висновків для вдосконалення методики правової кваліфікації цифрових правопорушень і підвищення ефективності правозастосовної діяльності.

Ключові слова: *протиправна поведінка, правова система, національна безпека, правозастосування, кіберправопорушення, інформаційні технології, кваліфікація, цифрові докази, кримінальне право.*

Tetruev Kirill. **Illegal behavior in the field of information technologies: approaches to understanding**

The article provides a theoretical and legal analysis of illegal behavior in the field of information technologies as a complex multi-phase and hybrid legal phenomenon that is formed in the conditions of digitalization of social relations. The limitations of traditional criminal law approaches to the qualification of digital acts, which do not take into account their procedural dynamics, algorithmic mediation and masking mechanisms, are substantiated. A conceptual model of the structure of cybercrime is proposed, which reflects the sequence of its phases and allows to clarify the boundaries of subjectivity, the objective side and the degree of social danger. The practical significance of the study lies in the possibility of using the conclusions obtained to improve the methodology for the legal qualification of digital offenses and increase the efficiency of law enforcement activities.

Keywords: *unlawful conduct, legal system, national security, law enforcement, cybercrime, information technology, qualification, digital evidence, criminal law.*

** **Tetruev Kirill,** Postgraduate Student of Koretsky Institute of State and Law of the NAS of Ukraine*

Вступ. Стрімкий розвиток інформаційних технологій та їх всеохопна інтеграція у суспільні, економічні й управлінські процеси зумовили глибинні трансформації правової реальності. Цифровізація не лише розширила можливості комунікації, обігу інформації та автоматизації діяльності, але й сформувала якісно новий простір для виникнення, модифікації та еволюції протиправної поведінки. У цих умовах традиційні правові конструкції, вироблені для регулювання суспільних відносин у фізичному середовищі, дедалі частіше виявляються недостатніми для адекватного осмислення та кваліфікації діянь, що здійснюються із застосуванням цифрових технологій. Протиправна поведінка у сфері інформаційних технологій характеризується підвищеним рівнем складності, багаторівневістю та гібридністю, що зумовлено поєднанням технічних, інформаційних і поведінкових компонентів. На відміну від класичних правопорушень, цифрові діяння нерідко не мають чітко окреслених просторових і часових меж, здійснюються опосередковано через алгоритмічні системи та розподілену мережеву інфраструктуру, а їх наслідки можуть проявлятися із затримкою або в множинних юрисдикціях. Це істотно ускладнює не лише виявлення та фіксацію таких діянь, але й їх правову інтерпретацію, встановлення суб'єктного складу та оцінку ступеня суспільної небезпеки.

Особливої актуальності проблема набуває в умовах зростання ролі кіберпростору як критично важливого елементу національної безпеки. Інформаційні системи та цифрові ресурси дедалі частіше стають об'єктами цілеспрямованого протиправного впливу, наслідком якого є порушення функціонування інфраструктури, витік конфіденційних даних, маніпуляція інформацією та завдання значної шкоди публічним і приватним інтересам. У цьому контексті протиправна поведінка у сфері інформаційних технологій виходить за межі суто технічної проблематики та набуває системного правового значення, вимагаючи комплексного наукового осмислення. Разом із тим у правовій доктрині відсутній усталений підхід до розуміння сутності та структури такої поведінки. Наявні дефініції та класифікації здебільшого фрагментарно відображають окремі аспекти цифрових правопорушень, концентруючись або на технічному способі їх вчинення, або на формально-юридичних ознаках, закріплених у кримінальному законодавстві. Такий підхід не дозволяє повною мірою врахувати процесуальний характер кібердіянь, їх фазовість, алгоритмічну опосередкованість та маскувальні механізми, що є визначальними для сучасної протиправної активності у цифровому середовищі. У зв'язку з цим постає об'єктивна потреба у виробленні оновлених наукових підходів до розуміння протиправної поведінки у сфері інформаційних технологій як складного правового феномена, що розвивається у динамічному техніко-інформаційному середовищі. Таке переосмислення має ґрунтуватися на поєднанні кримінально-правового, криміналістичного та інформаційно-аналітичного аналізу, забезпечуючи методологічну цілісність і придатність отриманих висновків для практики правозастосування. Саме в

цьому контексті обрана тема статті є актуальною, теоретично значущою та практично необхідною для подальшого розвитку правової науки й удосконалення механізмів реагування на виклики цифрової епохи.

У межах загальнотеоретичного правового аналізу протиправна поведінка традиційно розглядається як форма соціально значущої девіації, що суперечить нормативно встановленим моделям належної поведінки та посягає на охоронювані державою суспільні відносини. Теорія держави і права виходить із того, що протиправність не зводиться виключно до формального порушення правової норми, а є складною соціально-юридичною категорією, яка поєднує нормативний, ціннісний і поведінковий виміри. Саме ця багатовимірність дозволяє розглядати протиправну поведінку як результат взаємодії об'єктивних регуляторних обмежень і суб'єктивного волевиявлення особи в конкретному соціальному середовищі.

У цифровому просторі класичні теоретико-правові уявлення про протиправність зазнають суттєвої трансформації. Інформаційні технології опосередковують поведінку суб'єкта, змінюють механізми реалізації волі та ускладнюють безпосередній причинно-наслідковий зв'язок між дією і шкідливим результатом. За таких умов протиправність втрачає характер миттєвого акту порушення норми та набуває рис процесуального феномена, що розгортається у часі та просторі через низку взаємопов'язаних дій, технічних операцій і алгоритмічних рішень.

Огляд літератури. У міжнародній науковій традиції питання дефініційних та класифікаційних проблем кіберзлочинності було предметом низки оглядових праць, що систематизували феноменологію і типологію правопорушень у цифровому середовищі та підкреслювали розрив між технічною складністю діянь і традиційними кримінально-правовими категоріями. Зокрема, у ретельних оглядах літератури й узагальненнях практики підкреслюється необхідність розмежування кіберзалежних, кібер-зумовлених та кібер-асистованих правопорушень, а також наголошується на труднощах у застосуванні класичних конструкцій умислу, закінченості діяння і місця вчинення злочину в умовах децентралізованої інфраструктури мережі Інтернет. Ці універсальні висновки лягли в основу подальших спеціалізованих праць і практичних рекомендацій щодо адаптації правових норм до цифрової реальності[3].

Практико-орієнтовані міжнародні ініціативи й аналітичні звіти, зокрема оцінки впливу Будапештської конвенції, демонструють, що імплементація міжнародних стандартів сприяє унормуванню підходів до криміналізації окремих форм кіберзлочинності та процедур отримання електронних доказів, водночас вказуючи на постійні проблеми процесуальної сумісності, оперативно-технічної підготовки слідчих та механізмів транснаціональної співпраці. Ці висновки становлять нормативно-методологічну основу реформ, проте конкретні механізми імплементації і практика їх застосування в національних правових системах потребують додаткового емпіричного й

теоретичного аналізу[4]. У національному контексті останні публікації українських науковців і практиків концентрують увагу на системних прогалинах у статистиці, організації розслідування та законодавчій класифікації кіберзлочинів. Аналітичні огляди стану запобігання кіберзлочинності та посібники з цифрових доказів фіксують нестачу уніфікованих процедур документування цифрових слідів, проблеми з ідентифікацією суб'єкта в мережі та невідповідність частин Кримінального кодексу України сучасним технологічним ризикам. Окремі дослідження вказують на потребу підвищення технічної компетентності слідчих і створення спеціалізованих підрозділів для ефективної розв'язки кіберсправ[1]. Незважаючи на значний масив праць, що окреслюють проблему, у науковому полі залишаються суттєві невирішені питання, котрі становлять предмет цієї статті. По-перше, відсутня завершена методологія формалізованої кваліфікації гібридних діянь, які одночасно містять ознаки кіберзалежних і кібер-зумовлених правопорушень, що ускладнює ідентифікацію складу злочину та застосування санкцій. По-друге, не вироблено адекватних критеріїв для встановлення суб'єктності в анонімізованому середовищі: традиційні докази і процесуальні приписи часто не дозволяють однозначно пов'язати дію з конкретною фізичною особою або юридичним суб'єктом. По-третє, нормативно-процесуальні колізії між положеннями національного кримінального законодавства та міжнародно-процедурними інструментами ускладнюють оперативність і ефективність транснаціонального розслідування. І нарешті, лишається недостатньо розробленою проблематика допустимості та автентичності цифрових доказів у судовій практиці з огляду на їхню вразливість до маніпуляцій і технічних артефактів.

Постановка проблеми дослідження. Розвиток інформаційних технологій та стрімка цифровізація суспільних процесів призвели до формування нового середовища, у якому протиправна поведінка набуває специфічних форм і властивостей. Цифровий простір породжує особливі ризики, пов'язані з високою швидкістю поширення інформації, транснаціональністю комунікацій, доступністю анонімних та технічно складних інструментів для вчинення правопорушень. У таких умовах державні інституції стикаються з об'єктивними труднощами у виявленні, фіксації та кваліфікації діянь, що відбуваються у кіберсфері. Українська правова система, попри значний поступ у сфері кібербезпеки та приведення законодавства у відповідність до міжнародних стандартів, усе ще не забезпечує достатньої визначеності правових категорій, що ускладнює правозастосування та породжує ризики для ефективного правового реагування[5].

З позицій теорії держави і права принциповим є розмежування понять «протиправна поведінка», «правопорушення» та «злочин», оскільки протиправність виступає первинною юридичною ознакою, яка передує кримінально-правовій оцінці. Протиправна поведінка охоплює ширше коло діянь, ніж кримінально карані акти, і включає всі форми порушення нормативних приписів незалежно від рівня їх суспільної небезпеки та виду юридичної відпо-

відальності. У цифровому середовищі це розмежування набуває особливої ваги, оскільки значна частина шкідливих інформаційних впливів не завжди одразу підпадає під ознаки складу злочину, проте вже становить загрозу стабільності правового порядку.

Теоретико-правова доктрина також наголошує на тому, що протиправність поведінки є результатом нормативної оцінки, яка залежить від рівня розвитку правової системи, стану законодавства та здатності держави ефективно регулювати нові суспільні відносини. В умовах стрімкого технологічного розвитку виникає нормативний розрив між фактичними моделями цифрової поведінки та їх правовим осмисленням, що зумовлює появу «сірих зон» правового регулювання. Саме в цих зонах протиправна поведінка у сфері інформаційних технологій набуває латентного та гібридного характеру, ускладнюючи її ідентифікацію та правову кваліфікацію.

Проблема кваліфікації протиправної поведінки у сфері інформаційних технологій має фундаментальний міждисциплінарний характер. Вона лежить на перетині кримінального права, криміналістики, кібербезпеки, інформаційного права та процесуального доказування. Її вирішення потребує наукового обґрунтування понять, які досі залишаються дискусійними, зокрема «несанкціонований доступ», «втручання в роботу інформаційних систем», «цифровий слід», «віртуальний простір», «ідентифікація суб'єкта». У роботах зарубіжних дослідників, таких як S.Brenner1, T. Holt, A. Bossler та K.Seigfried-Spellar1, акцентовано на тому, що традиційні кримінально-правові підходи не враховують багатовимірності кіберсередовища, тоді як українські автори (Ю. Максименко[7], А. Кирилюк[4]) наголошують на потребі оновлення теоретичної бази та адаптації кримінально-правових норм до реалій кіберпростору. Актуальність проблеми зумовлена також практичними потребами: зростанням кількості кіберзлочинів, складністю їх документування, проблемами встановлення особи правопорушника, міжнародною юрисдикційною фрагментованістю та обмеженою можливістю проведення ефективних слідчих дій у транснаціональних справах. Усе це створює необхідність системного наукового аналізу та вироблення уніфікованих підходів до розуміння й кваліфікації протиправної поведінки у сфері цифрових технологій. Вирішення цих завдань є критично важливим не лише для розвитку вітчизняної кримінально-правової доктрини, але й для забезпечення національної безпеки, стабільності інформаційного простору та підвищення ефективності правозастосовної діяльності.

Мета та завдання дослідження. Метою статті є теоретичне й методологічне переосмислення підходів до визначення та кваліфікації протиправної поведінки у сфері інформаційних технологій, спрямоване на формування оновленої концептуальної моделі, здатної відобразити складність і багаторівневість сучасних кібердіянь. На відміну від усталених підходів, які зосереджуються переважно на класифікації кіберзлочинів за їх технічною природою або за ознаками, закріпленими у кримінальному законодавстві, дана

стаття пропонує розглядати цифрове правопорушення як динамічний правовий феномен, що поєднує технічні, інформаційні та поведінкові компоненти, взаємодія яких визначає характер суспільної небезпеки й особливості юридичної оцінки.

Для реалізації поставленої мети сформульовано низку взаємопов'язаних завдань. По-перше, здійснити критичний аналіз чинних кримінально-правових і криміналістичних підходів до кваліфікації діянь у сфері цифрових технологій з ідентифікацією їх системних обмежень. По-друге, дослідити особливості технологічних процесів, що визначають специфіку протиправної поведінки в кіберпросторі, та встановити, які з них потребують окремого правового реагування або уточнення в законодавстві. По-третє, розробити концептуальні критерії, здатні забезпечити більш точну ідентифікацію суб'єкта, об'єктивної сторони та межі закінченості кіберправопорушення з урахуванням його гібридного характеру. По-четверте, запропонувати науково вмотивовані рекомендації для удосконалення національної моделі кваліфікації таких діянь.

Виклад основного матеріалу. У межах теорії держави і права протиправна поведінка розглядається як структурований юридичний феномен, що включає суб'єкта, об'єкт, об'єктивну та суб'єктивну сторони, які перебувають у системному взаємозв'язку. Застосування цієї конструкції до цифрових правопорушень виявляє її обмеженість, оскільки у сфері інформаційних технологій зазначені елементи нерідко набувають розмитого або опосередкованого характеру. Зокрема, об'єкт посягання може мати нематеріальну природу, суб'єкт – бути частково анонімізованим або колективним, а об'єктивна сторона – реалізовуватися через автоматизовані технічні процеси. З огляду на це протиправність у кіберпросторі доцільно розглядати не лише як статичний факт порушення правової норми, а як динамічний процес, у межах якого юридично значущі ознаки формуються поступово. Такий підхід узгоджується з положеннями загальної теорії правопорушення, згідно з якими соціальна шкідливість та протиправність поведінки можуть накопичуватися внаслідок серії взаємопов'язаних дій, кожна з яких окремо не завжди досягає порогу кримінальної караності. У цифровому середовищі ця особливість проявляється особливо виразно, що обґрунтовує необхідність багатофазної моделі аналізу протиправної поведінки.

Дослідження сучасної протиправної поведінки у сфері інформаційних технологій зумовлює потребу у системному перегляді традиційних кримінально-правових уявлень про її природу. Проведений аналіз законодавства, судової практики та наукових джерел засвідчує, що правопорушення у кіберпросторі характеризуються багатовимірністю, динамічністю та гібридністю, що значною мірою ускладнює їх кваліфікацію. Чинна модель кримінально-правової оцінки кібердіянь, побудована на статичних формальних ознаках, не відображає реальної структури цифрового правопорушення, оскільки останнє нерідко поєднує у собі технічну дію, інформаційний вплив, маніпу-

лятивні стратегії та алгоритмічну поведінку системи. Одним із ключових наукових результатів стало формування концептуальної моделі багаторівневої структури протиправної поведінки у сфері ІТ, яка дає змогу диференціювати склад діяння залежно від поєднання технічних та інформаційно-комунікативних характеристик. Застосована методологія системного аналізу дала можливість простежити, що цифрове правопорушення нерідко виникає не як одноразова дія, а як процес, що складається з послідовних фаз: підготовки, ініціювання, взаємодії з інформаційною системою, маскування та розповсюдження наслідків. Саме виявлення цієї багатофазності стало важливим особистим науковим внеском автора, що уможливило уточнити межі закінченості кіберзлочину та його кваліфікаційні орієнтири[1]. Для ілюстрації запропонованого підходу представимо схему, яка відображає структуру цифрового протиправного діяння та взаємозв'язки його елементів *(рис. 1)*.

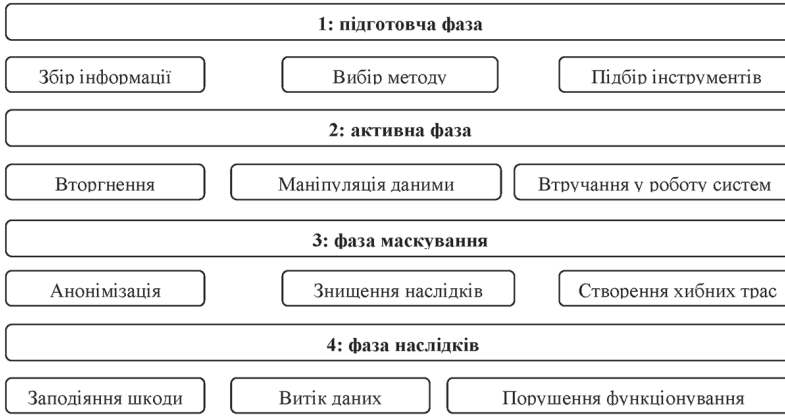

Рис. 1. Багаторівнева структура протиправної поведінки у сфері інформаційних технологій

Джерело: сформовано автором на основі[9]

Також слід підкреслити, що емпіричне вивчення судових рішень та оперативних матеріалів, що дало змогу виокремити найбільш поширені типи цифрових правопорушень та визначити їх правову природу. Унаслідок аналізу отримано фактичні дані, що узагальнені у *таблиці 1*, яка демонструє взаємозв'язок між технічною складністю діяння та ймовірністю виникнення проблем у його кваліфікації.

Таблиця 1

Залежність складності кваліфікації від технічної складності кіберправопорушення

Рівень технічної складності	Типові діяння	Ймовірність помилок у кваліфікації
Низька	Фішинг, прості шахрайства	Середня
Середня	Несанкціонований доступ, модифікація даних	Висока
Висока	DDoS, складні атаки на інфраструктуру, алгоритмічні маніпуляції	Дуже висока

Джерело: сформовано автором на основі[2]

Дослідження продемонструвало чітку тенденцію: із зростанням технічної складності кібердіяння зростає кількість правозастосовних помилок, що пов'язано з недостатністю криміналістичних інструментів, недосконалістю законодавчої термінології та обмеженою цифровою компетентністю осіб, які здійснюють розслідування.

Слід також акцентувати увагу на встановленні тенденцій зміни структури кіберзлочинності в Україні за останні роки. На основі узагальнення даних судової статистики та аналітичних звітів було побудовано графік *(рис. 2),* який дозволяє візуалізувати зростання категорії складних цифрових діянь.

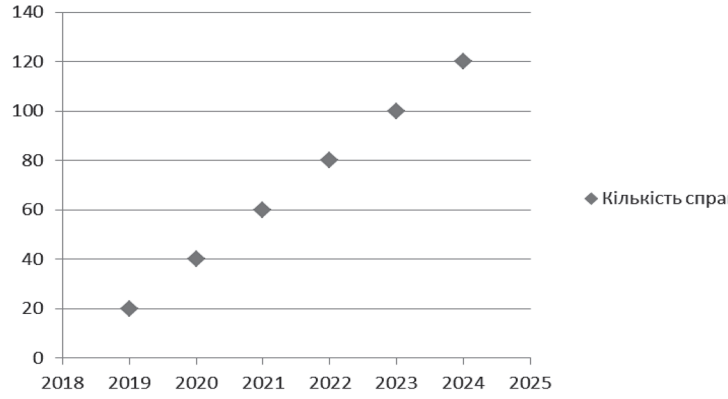

Рис. 2. Динаміка збільшення складних кіберправопорушень (умовні індексні дані)

Джерело: побудовано автором на основі[2]

Зазначені дані демонструють стійку тенденцію зростання кількості складних кібердіянь, що вчиняються із застосуванням багатокомпонентних технічних інструментів, а також свідчить про збільшення частки злочинів, пов'язаних із алгоритмічними атаками, використанням шкідливих програм нового покоління та маніпуляцією цифровими активами. Виявлена закономірність підтверджує ключову тезу дослідження: кваліфікація цифрових правопорушень потребує адаптивної моделі, яка враховує їх еволюцію та технічний розвиток[8].

Проведений аналіз дав змогу підкреслити необхідність оновлення методики кваліфікації кіберправопорушень, що полягає у необхідності поєднання кримінально-правової оцінки з техніко-інформаційним аналізом структури діяння та необхідності у розробленні критеріїв гібридизації, які уможливлюють відрізняти традиційні цифрові правопорушення від таких, що містять елементи складної технічної або когнітивної взаємодії, зокрема: ступінь алгоритмічної автономності дії, рівень децентралізації, інтенсивність цифрового маскування та кількість фаз, через які проходить діяння[6].

Таким чином, запропонована модель матиме концептуальне значення для формування нових підходів до правової кваліфікації протиправної поведінки у сфері інформаційних технологій. Виявлені тенденції, закономірності та встановлені зв'язки дають змогу не лише розширити теоретичну базу дослідження кіберзлочинності, але й удосконалити практику правозастосування.

Отже, залучення положень теорії держави і права дає змогу розширити розуміння протиправної поведінки у сфері інформаційних технологій за межі вузького кримінально-правового підходу. Протиправність постає як системна характеристика поведінки в умовах цифрового середовища, що формується на перетині нормативних заборон, технологічних можливостей і поведінкових стратегій суб'єкта. Це зумовлює необхідність адаптації класичних теоретичних конструкцій до реалій кіберпростору та створення гнучких моделей правового аналізу, здатних відобразити складність сучасних цифрових правопорушень.

Висновки. Проведене дослідження дає змогу сформувати раціонально обґрунтовану та внутрішньо логічну концепцію аналізу протиправної поведінки у сфері інформаційних технологій, що відповідає сучасним методологічним вимогам і базовим принципам правової науки. Слід зазначити, що цифрові правопорушення не можуть бути коректно оцінені в межах традиційних кримінально-правових моделей, оскільки у своїй сутності вони становлять багатофазні, техніко-інформаційні та поведінково зумовлені процеси. Такий висновок є логічно несуперечливим і підтверджений аналізом фактичних даних, зокрема статистичних показників та тенденцій розвитку складних форм кібердіяльності.

Розроблення авторської моделі багаторівневої структури цифрового правопорушення, ґрунтується на концептуально виваженому поєднанні кримінально-правового, криміналістичного та інформаційно-аналітичного підхо-

дів. Відмінність цієї моделі від існуючих полягає у її здатності раціонально відображати внутрішню динаміку кібердіяння, чітко виокремлюючи фази підготовки, активної дії, маскування та формування наслідків. Запропонована структура є достовірною, оскільки спирається на практичний аналіз цифрових інцидентів та узагальнення слідчих матеріалів; вона також узгоджується з науковими принципами системності, причинності та об'єктивності.

Критерії гібридизації кіберправопорушень сформульовані на основі системного аналізу технологічних і правових характеристик цифрових діянь. Ці критерії є раціональними за своєю структурою, несуперечливими за логікою побудови та придатними для практичного використання. Їх значення полягає у можливості застосування для уточнення меж суб'єктності, об'єктивної сторони та ступеня суспільної небезпеки у складних кіберсправах.

Практичне значення дослідження полягає у можливості використання отриманих результатів для вдосконалення методики кваліфікації цифрових правопорушень, розроблення ефективних алгоритмів аналізу електронних доказів та підвищення компетентності суб'єктів правозастосування.

1. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: дис. … канд. юрид. наук: 12.00.08 / НАН України; Інститут держави і права ім. В. М. Корецького. Київ, 2002. 212 с. **2.** Гончар Т. О., Стрельцов Є. Л. Кримінальне право України. Загальна та особлива частини: навч. посібник. Харків: Одісей, 2014. 240 с. **3.** Денисов С. Ф. Особа злочинця у кримінологічній теорії України. *Вісник Кримінологічної асоціації України.* 2020. № 1 (22). С. 152–159. DOI: https://doi.org/10.32782/2524-0374/2022-11/146 **4.** Кирилюк А. В. Поняття та види інформаційних правопорушень. *Часопис цивілістики.* 2017. Вип. 26. С. 51–55. **5.** Кормич Б. А. Інформація як категорія інформаційного права. *Актуальні проблеми держави і права.* Вип. 16. Одеса: Юридична література, 2002. С. 367–374. **6.** Лисько Т. Д., Меланіч В. В., Славіта Ю. В. Протидія кіберзлочинності: сучасний стан вітчизняного законодавства та досвід зарубіжних країн. *Актуальні проблеми держави і права.* 2022. № 96. С. 44–49. DOI: https:// doi.org/10.32782/apdp.v96.2022.4. **7.** Максименко Ю.Є. Інформаційні правопорушення: поняття та ознаки. *Глобальна організація союзницького лідерства.* 2014. С. 42–56. URL: http://www.goal-int.org **8.** Малій М. І. Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження: дис. ... канд. юрид. наук: 12.00.08. Хмельницький, 2021. 213 с. **9.** Тихомиров О. О. Інформаційні правопорушення: теоретико-правова концепція. *Інформаційна безпека людини, суспільства, держави.* 2015. № 1 (17). С. 38–47.

References

1. Azarov, D. S. (2002). Criminal liability for crimes in the field of computer information: dissertation ... candidate of law: 12.00.08 / NAS of Ukraine; Institute of State and Law named after V. M. Koretsky. Kyiv, 212. **2.** Gonchar, T. O., Streltsov, E. L. (2014). Criminal law of Ukraine. General and special parts: textbook. Kharkiv: Odyssey, 240. **3.** Denisov, S. F. (2020). The person of a criminal in the criminological theory of Ukraine. *Bulletin of the Criminological Association of Ukraine,* № 1 (22), 152–159. DOI: https://doi.org/10.32782/2524-0374/2022-11/146 **4.** Kyrylyuk, A. V. (2017). The concept and types of information offenses. *Journal of Civil Studies,* Issue 26, 51–55. **5.** Kormych, B. A. (2002).

Information as a Category of Information Law. Current Problems of the State and Law. Issue 16. Odesa: Legal Literature, 367–374. **6.** Lysko, T. D., Melanich, V. V., Slavita, Yu. V. (2022). Combating Cybercrime: Current State of Domestic Legislation and Experience of Foreign Countries. *Current Problems of the State and Law,* № 96, 44–49. DOI: https:// doi.org/10.32782/apdp.v96.2022.4. **7.** Maksymenko, Yu.E. (2014). Information Offenses: Concepts and Signs. *Global Alliance Leadership Organization,* 42–56. URL: http://www.goal-int.org **8.** Maliy, M. I. (2021). The person of a computer criminal as an object of criminological research: dissertation ... candidate of law: 12.00.08. Khmelnytskyi, 213. **9.** Tikhomirov, O. O. (2015). *Information crimes: theoretical and legal concept. Information security of man, society, state,* № 1 (17), 38–47.

Tetruev Kirill. Illegal behavior in the field of information technologies: approaches to understanding.

The rapid development of information technologies and the deep digitalization of social relations have fundamentally transformed the nature of unlawful conduct, giving rise to new forms of illegal activity in cyberspace. Traditional legal concepts, designed for acts committed in the physical world, increasingly fail to adequately capture the dynamic, multi-layered and technologically mediated character of offenses carried out through digital infrastructures.

The aim of the article is to provide a theoretical and methodological rethinking of approaches to understanding and qualifying unlawful behavior in the field of information technologies, with a focus on overcoming the limitations of formalistic and purely technical classifications of cyber offenses.

The article substantiates that unlawful conduct in the IT sphere should be conceptualized as a complex, multi-phase and hybrid process combining technical actions, information influence and behavioral strategies. A conceptual model of cyber offense structure is developed, which identifies successive phases of preparation, active impact, masking and formation of consequences. It is demonstrated that the growth of technical complexity and algorithmic mediation of digital acts directly correlates with an increased risk of errors in legal qualification, particularly in determining subjectivity, the moment of completion of the offense and the degree of social harm. The research also formulates criteria for identifying the hybrid nature of digital offenses, taking into account the level of algorithmic autonomy, decentralization, masking techniques and procedural dynamics.

The study concludes that effective qualification of unlawful behavior in the field of information technologies requires an adaptive legal model that integrates criminal law analysis with technical and informational assessment of digital processes. The proposed approach contributes to the development of a more accurate and systematic understanding of cyber offenses and can be used to improve law enforcement practices, the evaluation of digital evidence and the overall effectiveness of criminal law responses to contemporary cyber threats.

Keywords: *unlawful conduct, legal system, national security, law enforcement, cybercrime, information technology, qualification, digital evidence, criminal law.*

Дата першого надходження рукопису до видання: 08.01.2026
Дата прийнятого до друку рукопису після рецензування: 03.03.2026
Дата публікації: 24.03.2026