DOI https://doi.org/10.36059/978-966-397-651-8-34

ЦИФРОВА КРИМІНАЛІСТИКА У ВИЩІЙ ОСВІТІ: ПІДГОТОВКА ФАХІВЦІВ ДО РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ У ПЕРІОД ВОЄННОГО СТАНУ

Козак Наталія Володимирівна
кандидат юридичних наук, доцент,
доцент кафедри права
Луцький національний технічний університет
м. Луцьк, Україна

Збройна агресія російської федерації проти України та введення правового режиму воєнного стану зумовили необхідність кардинального переосмислення концептуальних засад криміналістичної науки й правозастосовної практики в частині нормативно-правового регулювання протидії кіберзагрозам [1], безпрецедентна за інтенсивністю та систематичністю ворожа активність у кіберпросторі, спрямована проти об'єктів критичної інфраструктури, державних інформаційних систем і цивільного населення, актуалізує питання вироблення ефективного криміналістичного інструментарію, що відповідає сучасним викликам кримінального провадження в умовах збройного конфлікту [2]. Зазначена проблематика набуває особливої правової значущості з огляду на необхідність забезпечення процесуальної допустимості доказів, отриманих у результаті досудового розслідування кіберправопорушень і воєнних злочинів, вчинених із застосуванням інформаційно-комунікаційних технологій [2].

Всеосяжне проникнення цифрових технологій у сфери суспільного та державного функціонування зумовило перетворення електронної інформації на невід'ємний структурний елемент як об'єктивної сторони кримінального правопорушення, так і доказової бази в межах кримінального провадження [3]. За таких обставин першочергового значення набуває розроблення принципово нових криміналістичних концепцій, що органічно поєднують правові механізми з технологічними засобами документування *locus delicti* та *corpus delicti* у цифровому середовищі, з неухильним дотриманням вимог щодо збереження ланцюга зберігання доказів (*chain of custody*) та встановлення суб'єкта кримінального правопорушення [2]. Правовий режим воєнного стану формує безпрецедентний суспільний запит на висококваліфікованих фахівців у галузі цифрової криміналістики, на яких покладається завдання юридично коректної кваліфікації кримінального правопорушення, своєчасної фіксації

кіберправопорушень і забезпечення відповідності матеріалів досудового розслідування вимогам процесуальної допустимості та допустимості доказів у судовому провадженні [2].

Цифрова криміналістика конституювалася як самостійна галузь юридичної науки, предметом якої є методологічно обґрунтована сукупність прийомів і методів пошуку, фіксації, збереження, дослідження та процесуального представлення електронних доказів у межах кримінального провадження. Основним об'єктом криміналістичного пізнання у зазначеній галузі виступає цифровий слід (*digital footprint*) – структурована сукупність комп'ютерних даних, що утворюється внаслідок взаємодії суб'єкта кримінального правопорушення або інших учасників кримінально значущих відносин з електронними пристроями, автоматизованими системами та інформаційно-телекомунікаційними мережами і становить невід'ємний елемент об'єктивної сторони інформаційних правопорушень [3].

Динамічне розширення масштабів кіберзлочинності – зокрема несанкціонованого втручання в роботу електронно-обчислювальних систем, незаконного заволодіння персональними даними, протиправних маніпуляцій із засобами електронних платежів та розповсюдження шкідливого програмного забезпечення – зумовлює формування стійкого та зростаючого дефіциту фахівців, спроможних здійснювати кваліфіковану роботу з електронними доказами у суворій відповідності до вимог нормативно-правового регулювання, встановлених кримінальним процесуальним законодавством і міжнародними криміналістичними стандартами [1]. Вирішення зазначеної проблеми набуває особливої актуальності в контексті правового режиму воєнного стану, що істотно ускладнює організаційно-процесуальні умови провадження слідчих і оперативно-розшукових дій у кіберпросторі [2].

Переосмислення концептуальних засад криміналістичної освіти об'єктивно зумовлює необхідність переорієнтації освітнього процесу на формування цифрових компетентностей у широкому колі суб'єктів кримінального провадження – зокрема, слідчих, прокурорів, детективів, спеціалістів-криміналістів та судових експертів. Здатність уповноважених суб'єктів правоохоронної діяльності до кваліфікованого застосування цифрових інструментів визнається визначальною умовою забезпечення належної якості досудового розслідування та судового розгляду справ, кваліфікація кримінального правопорушення у яких пов'язана з протиправними діяннями у кіберпросторі. Рівень цифрової правової грамотності безпосередньо детермінує процесуальну допустимість і доказову силу електронних матеріалів, отриманих під час досудового розслідування [3].

У цьому контексті обґрунтовується нагальна потреба у запровадженні спеціалізованої освітньої програми, спрямованої на підготовку «цифрового криміналіста» як самостійної кваліфікаційної категорії фахівців, що функціонують на перетині юридичних і технічних галузей знань. Метою відповідної програми є формування фахівця, компетентного в обох сферах та спроможного належним чином здійснювати покладені на нього функції на кожному з етапів кримінального провадження – від збирання та фіксації первинної доказової бази до її представлення в судовому засіданні з дотриманням усіх вимог щодо ланцюга зберігання . Нормативно-правове регулювання відповідної кваліфікаційної категорії, у свою чергу, має забезпечувати однозначне визначення правового режиму діяльності цифрового криміналіста в системі органів кримінальної юстиції [2].

Першочерговим завданням у сфері методологічного забезпечення залишається розроблення науково виваженої моделі організації виявлення й розслідування кіберзлочинів, що охоплювала б систему методів отримання доказів із відкритих і закритих цифрових джерел у суворій відповідності до процесуальних норм, які визначають їхню допустимість [2]. Визначення об’єктивної сторони кожного виду кіберзлочину з урахуванням специфіки цифрового *locus delicti* та встановлення *corpus delicti* в умовах розподіленого цифрового середовища становлять окремі дослідницькі проблеми, що потребують міждисциплінарного осмислення [5]. Невід’ємним складником фахової підготовки має стати розвиток навичок доступного та юридично грамотного викладу технічних висновків цифрової експертизи перед судовою аудиторією, що є необхідною запорукою процесуальної допустимості доказів і ефективної міждисциплінарної взаємодії в системі кримінального судочинства [

Всебічна реформа змістовного наповнення та методологічних засад підготовки фахівців у галузі цифрової криміналістики в умовах правового режиму воєнного стану є невід’ємною передумовою досягнення належного рівня процесуальної компетентності суб’єктів кримінального провадження. Орієнтація навчальних програм на положення Будапештської конвенції про кіберзлочинність та відповідні документи Організації Об’єднаних Націй уможливлює вироблення уніфікованих підходів до поводження з електронними доказами в межах транскордонних проваджень, забезпечуючи тим самим нормативно-правове регулювання, узгоджене з міжнародними стандартами допустимості доказової бази та засадами взаємної правової допомоги у сфері цифрових розслідувань [1].

В умовах правового режиму воєнного стану пріоритетного значення набуває практична спрямованість підготовки: відпрацювання

проваджень, пов'язаних із шахрайством із використанням криптовалют, проявами кібертероризму та масштабним збором цифрових доказів засобами розвідки на основі відкритих джерел , що безпосередньо сприяє документуванню воєнних злочинів із дотриманням принципу chain of custody та забезпеченню принципу невідворотності покарання [4]. Стратегічним орієнтиром вищої юридичної освіти України в нинішніх умовах є формування аналітично мислячих і технічно компетентних фахівців, спроможних забезпечувати процесуальну допустимість електронних доказів та ухвалювати обґрунтовані процесуальні рішення в умовах дефіциту часу й динамічних змін у характері кіберзагроз [6].

Література

1. Конвенція про кіберзлочинність (Будапештська конвенція) : Рада Європи від 23.11. 2001 р. (ратифікована Законом України від 07.09.2005 р. № 2824-IV). URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 17.08.2026).
2. Кримінальний процесуальний кодекс України : Закон України від 13.04. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 17.08.2026).
3. Петрик В. В. Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. Вип. 87, ч. 4. С. 115–121. DOI: https://doi.org/10.24144/2307-3322.2025.87.4.17
4. Погорецький М. А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів і злочинів проти основ національної безпеки: методи OSINT. *Вісник кримінального судочинства.* 2023. № 3–4. С. 84–102. URL: https://vkslaw.knu.ua/ (дата звернення: 17.08.2026).
5. Шепітько В. Ю., Шепітько М. В., Латіш К. В., Капустіна М. В., Демидова Ю. Цифрова злочинність і її роль у формуванні інформації, заснованої на доказах, у свідомості військових операцій. [Б. м.] : Exlibrus, 2025.
6. Квашук О. Д. Використання електронних доказів у кримінальному провадженні. *Центральноукраїнський вісник права та публічного управління.* 2025. № 2. С. 34–41. DOI: https://doi.org/10.32840/cuj-2025-2-5