реагування на надзвичайні події, дозволяючи координувати дії різних служб.

Європейський досвід свідчить, що інтеграція сучасних інформаційних технологій у діяльність силових структур сприяє підвищенню оперативності та ефективності боротьби зі злочинністю, а також дозволяє здійснювати аналіз даних у режимі реального часу.

Підсумовуючи можна сказати, що інформаційні технології та сучасні методи інформаційно-аналітичного забезпечення є невід'ємною складовою сучасної роботи силових структур як в Україні, так і в Європі. Україна активно впроваджує інноваційні рішення для модернізації своїх правоохоронних органів, інтегрує цифрові платформи та розширює міжнародну співпрацю. Європейський досвід демонструє, що завдяки високому рівню інтеграції, використанню штучного інтелекту та ефективним системам обміну інформацією, можна значно підвищити ефективність оперативного реагування та запобігання злочинності.

Порівнюючи практики, можна зробити висновок, що Україна має великий потенціал для подальшої цифровізації силових структур, а запозичення європейських технологічних рішень сприятиме більш ефективній протидії кримінальним правопорушенням. Водночас, подолання викликів у сфері кібербезпеки, інтеграції систем та гармонізації законодавства залишається пріоритетним завданням для забезпечення стійкості та ефективності сучасних аналітичних платформ.

Ольга Габорець,
доцент кафедри оперативно-розшукової діяльності
та інформаційної безпеки факультету №3
Донецького державного університету внутрішніх справ,
доктор філософії, доцент

Людмила Рибальченко,
доцент кафедри кібербезпеки та інформаційних технологій,
Університет митної справи та фінансів,
кандидат економічних наук доцент

ЦИФРОВА ІНФОРМАЦІЯ ТА ЦИФРОВІ ДОКАЗИ: ОЗНАКИ, ПОНЯТТЯ ТА ВІДМІННОСТІ

У сучасному цифровому середовищі правозастосовна практика дедалі частіше стикається з необхідністю оперувати даними, які існують винятково в електронній формі. Такі дані можуть бути як нейтральною цифровою інформацією, так і здатними набувати юридичного значення в межах кримінального провадження, трансформуючись у цифрові докази. У зв’язку з цим особливого значення набуває чітке розмежування понять «цифрова інформація» та «цифрові докази», що дозволяє забезпечити належну правову кваліфікацію таких об'єктів, визначити межі допустимості їх використання в доказуванні та унеможливити порушення процесуальних прав учасників

кримінального провадження. Відповідно до ст. 1 Закону України «Про інформацію» від 02.10.1992 р. № 2657-XII [1], інформацією вважаються будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Отже, цифрова інформація – це форма існування інформації, яка реалізується через числове кодування, що дозволяє її обробку за допомогою інформаційно-комунікаційних систем. Натомість кримінальне процесуальне право потребує від інформації додаткових юридичних властивостей, аби визнати її доказом. Стаття 84 Кримінального процесуального кодексу України (далі – КПК України) [2] визначає, що доказами в кримінальному провадженні є фактичні дані, отримані в передбаченому законом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність або відсутність обставин, які підлягають доказуванню. Такі дані можуть бути отримані, зокрема, із показань, речових доказів, документів, висновків експертів. Однак у чинному КПК України досі не закріплено самостійного процесуального джерела у вигляді цифрових або електронних доказів. Проте ч. 2 ст. 99 КПК України [2] відносить до документів комп'ютерні дані, вказуючи на можливість визнання певних цифрових об'єктів документами за своєю правовою природою. Водночас така класифікація не враховує специфічні ознаки цифрових даних: їх нематеріальний характер, можливість зберігання у хмарних сервісах, мультиплікованість, наявність метаданих, які потребують спеціальних технічних знань для ідентифікації автентичності та цілісності. Законопроєкт № 4004 від 31.08.2020 р. «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» [3] передбачає визначення електронних доказів як інформації в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ фактів або обставин у кримінальному провадженні. Аналогічне визначення містять також процесуальні кодекси цивільної та адміністративної юрисдикції (ч. 1 ст. 100 ЦПК України, ч. 1 ст. 99 КАС України, ч. 1 ст. 96 ГПК України). Конвенція про кіберзлочинність від 23.11.2001 р. (Будапештська конвенція), ратифікована Законом України № 2824-IV від 07.09.2005 р., у п. b ст. 1 визначає комп'ютерні дані як будь-яке представлення фактів, інформації або концепцій у формі, яка придатна для обробки комп'ютерною системою. Водночас електронні докази, на відміну від звичайних документів, можуть включати складові, які не є видимими або доступними для візуального сприйняття (зокрема, хеш-коди, лог-файли, GPS-координати тощо). У цьому полягає одна з головних відмінностей цифрових доказів – вони є даними, які потребують спеціального інструментарію для доступу, обробки та аналізу. Таким чином, цифрові докази характеризуються такими ознаками: створюються в цифровому середовищі або перетворюються в нього; існують у формі цифрових сигналів; зберігаються на електронних носіях або в хмарних системах; не мають матеріального вираження; можуть бути змінені або знищені без фізичного втручання; потребують технічної експертизи для встановлення автентичності. Отже, цифрова інформація – це загальна категорія, що включає будь-які відомості в цифровій формі, тоді як цифрові докази – це лише ті з них,

які мають значення для справи, отримані законним шляхом і допущені до провадження у межах кримінального процесу. Вони можуть бути документом (ч. 2 ст. 99 КПК), речовим доказом (ст. 98 КПК) або – за умови прийняття відповідних змін – самостійним джерелом доказів. Така класифікація має надзвичайно важливе значення для практики, зокрема для дотримання принципу допустимості доказів (ст. 86 КПК України) та забезпечення захисту права особи на справедливий суд [2].

Таким чином, у результаті проведеного дослідження встановлено, що цифрова інформація є основоположною категорією в умовах розвитку електронного середовища, проте не вся вона автоматично набуває доказового значення. Правова дійсність вимагає чіткого концептуального та процесуального розмежування між будь-якою цифровою інформацією та цифровими доказами як специфічною формою реалізації доказів у кримінальному провадженні.

Список використаних джерел

1. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2657-12 (дата звернення: 13.03.2025)

2. Кримінальний процесуальний кодекс України : Кодекс України; Закон, Кодекс від 13.04.2012 № 4651-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/4651-17 (дата звернення: 13.03.2025)

3. Проєкт закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів від 31 серпня 2020 р. № 4004. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511 =69771 (дата звернення: 13.03.2025)

Сергій Зеленський,
доцент кафедри оперативно-розшукової діяльності
та інформаційної безпеки факультету № 3
Донецького державного університету внутрішніх справ,
к.ю.н., с.н.с., доцент

ПОЛІГРАФ, ЯК ІНСТРУМЕНТ ЗЕБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: МОЖЛИВОСТІ, РИЗИКИ, ПЕРСПЕКТИВИ ВИКОРИСТАННЯ

В умовах стрімкого розвитку технологій та зростання загроз в інформаційній сфері постає питання підвищення рівня захисту конфіденційної інформації [1]. Одним із засобів у цьому напрямі є забезпечення інформаційної безпеки з використанням поліграфа – пристрою, що аналізує фізіологічні реакції людини для визначення правдивості відповідей на подразники, запитання.

Поліграф – багатоканальний програмний технічний засіб, призначений