DOI https://doi.org/10.36059/978-966-397-613-6-64

НОРМАТИВНО-ПРАВОВІ РАМКИ ВИКОРИСТАННЯ ЦИФРОВИХ ІНСТРУМЕНТІВ КРИМІНАЛЬНОГО АНАЛІЗУ

Василова Оксана Василівна
кандидат юридичних наук,
асистент кафедри кримінального права юридичного факультету,
Чернівецький національний університет імені Юрія Федьковича
м. Чернівці, Україна

Сучасний кримінальний аналіз у цифровому середовищі ґрунтується на комплексному використанні взаємопов'язаних технологічних рішень, які забезпечують повний цикл роботи з цифровою інформацією – від її отримання до формування аналітичних висновків, придатних для використання у кримінальному провадженні. Їх інтегроване застосування створює необхідні технологічні та процесуальні передумови для забезпечення обґрунтованості, достовірності та процесуальної допустимості результатів кримінального аналізу, що визначає їх ключову роль у сучасній системі інформаційно-аналітичного забезпечення правоохоронної діяльності.

З огляду на зазначене, використання цифрових інструментів кримінального аналізу має здійснюватися у межах визначених нормативно-правових рамок, що забезпечують законність, допустимість і доказову значущість результатів аналітичної діяльності. Відповідно, цифровізація кримінального аналізу повинна реалізовуватися з урахуванням процесуальних вимог кримінального процесуального законодавства, яке регламентує правові підстави, порядок та умови отримання, обробки, збереження і використання інформації у кримінальному провадженні. Дотримання зазначених вимог є необхідною передумовою забезпечення належності, допустимості та достовірності цифрової інформації як джерела доказів, а також гарантією можливості її використання у процесі доказування. Відповідно, особливого значення набуває забезпечення процесуальної форми роботи з цифровими даними, що передбачає належне документування всіх етапів їх отримання та обробки, фіксацію технічних характеристик використаних інструментів, а також створення умов для подальшої перевірки і відтворення отриманих результатів.

Особливого значення зазначені вимоги набувають в умовах правового режиму воєнного стану, який супроводжується внесенням змін до Кримінального процесуального кодексу України, зокрема запровадженням спеціального правового регулювання, передбаченого розділом

ІХ-1 та статтею 615 КПК України [1]. Окреслені нормативні положення спрямовані на забезпечення безперервності кримінального провадження в умовах підвищених ризиків втрати матеріалів, обмеженого фізичного доступу до документів і доказів, переміщення органів досудового розслідування, а також необхідності забезпечення оперативного реагування на кримінальні правопорушення. У таких умовах особливого значення набуває використання цифрових технологій, які забезпечують можливість дистанційного доступу до матеріалів кримінального провадження, їх збереження у захищених інформаційних системах і підтримання безперервності процесуальної діяльності незалежно від зовнішніх обставин.

Зазначені нормативні зміни обумовлюють необхідність впровадження технологічних рішень, спрямованих на забезпечення цілісності, доступності та захищеності цифрової інформації, що використовується у кримінальному провадженні, що включає використання спеціалізованих інформаційно-аналітичних систем, які забезпечують централізоване збереження даних, контроль доступу до них, фіксацію всіх операцій із цифровою інформацією та можливість відновлення даних у разі їх втрати або пошкодження. Даний підхід дозволяє мінімізувати ризики втрати доказової інформації та забезпечити належний рівень її процесуального захисту.

У зв’язку з цим цифровий кримінальний аналіз набуває особливого значення як інструмент забезпечення належного документування процесуальних дій, збереження цифрових доказів і підтримання безперервності ланцюга зберігання інформації. Його застосування дозволяє забезпечити фіксацію джерел походження цифрових даних, документування процедур їх обробки та збереження, а також створення умов для перевірки їх автентичності та цілісності, що, у свою чергу, забезпечує відповідність результатів кримінального аналізу вимогам кримінального процесуального законодавства та створює необхідні передумови для їх використання у процесі доказування.

Реалізація зазначених завдань обумовлює необхідність впровадження комплексних організаційно-технологічних заходів, зокрема процедур резервного копіювання цифрових даних, застосування механізмів контрольованого доступу до інформаційних ресурсів, використання захищених середовищ зберігання інформації та забезпечення можливості аудиту операцій із цифровими даними. Застосування таких механізмів дозволяє забезпечити належний рівень захисту інформації, її відтворюваність та процесуальну допустимість, що є необхідною умовою ефективного використання цифрового кримінального аналізу у кримінальному провадженні [2].

Важливим компонентом правового регулювання застосування цифрових інструментів кримінального аналізу є забезпечення захисту персональних даних, що обробляються у межах кримінального провадження. Закон України «Про захист персональних даних» визначає базові принципи обробки персональної інформації, включно з принципами законності, цільового обмеження, пропорційності, мінімізації обсягу даних і забезпечення їх безпеки. З огляду на те, що кримінальний аналіз передбачає обробку значних масивів персональних даних, у тому числі чутливих категорій інформації, архітектура відповідних інформаційно-аналітичних систем повинна передбачати впровадження механізмів рольового розмежування доступу, ведення журналів доступу до інформації, аудиту операцій обробки даних і контролю передачі інформації між інформаційними системами. Забезпечення зазначених вимог є необхідною умовою правомірного використання цифрових аналітичних інструментів і гарантією дотримання прав і свобод людини у процесі здійснення кримінального провадження [3]. Водночас транснаціональний характер сучасного інформаційного середовища обумовлює необхідність узгодження національних правових механізмів із міжнародними стандартами отримання та використання електронних доказів. У зв'язку з цим особливого значення набуває дотримання міжнародних процедур отримання електронних доказів, які регламентують порядок формування, направлення та виконання відповідних запитів до іноземних суб'єктів і міжнародних провайдерів інформаційних послуг. Практичні рекомендації міжнародних організацій підкреслюють необхідність забезпечення належної процесуальної форми отримання електронних доказів, що включає обґрунтування запиту, визначення його правових підстав і забезпечення можливості подальшої процесуальної перевірки отриманої інформації [4].

Подальший розвиток міжнародно-правового регулювання у зазначеній сфері пов'язаний із прийняттям Другого додаткового протоколу до Конвенції про кіберзлочинність, відкритого для підписання у 2022 році, який спрямований на вдосконалення механізмів міжнародного співробітництва та підвищення ефективності процедур отримання електронних доказів. Приєднання держав до зазначеного протоколу відображає тенденцію до уніфікації процедур доступу до електронних доказів і гармонізації національних правових систем із міжнародними стандартами. Для України це створює необхідність адаптації національних процедур кримінального аналізу до міжнародних вимог, зокрема у частині забезпечення належного документування процесу отримання цифрових даних, дотримання ланцюга зберігання доказів,

а також забезпечення пропорційності втручання у сферу приватності при отриманні та використанні електронної інформації [5].

Література:

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

2. Про внесення змін до Кримінального процесуального кодексу України щодо удосконалення порядку здійснення кримінального провадження в умовах воєнного стану : Закон України від 14.04.2022 № 2201-IX. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2201-20#Text

3. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

4. United Nations Office on Drugs and Crime. Electronic evidence. URL: https://www.unodc.org

5. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. *Council of Europe,* 2022. URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol

DOI https://doi.org/10.36059/978-966-397-613-6-65

СЕКРЕТНІСТЬ ДЖЕРЕЛА ІНФОРМАЦІЇ ТА ПРАВО НА ЗАХИСТ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ, ПОВ'ЯЗАНИХ ЗІ ЗБРОЙНИМ КОНФЛІКТОМ: МЕЖІ ВИКОРИСТАННЯ У ДОКАЗУВАННІ

Ганенко Ігор Сергійович
кандидат юридичних наук,
прокурор Херсонської окружної прокуратури Херсонської області
м. Херсон, Україна

У кримінальних провадженнях, пов'язаних зі збройним конфліктом, процесуальне значення має не сам режим обмеженого доступу до інформації, а те, чи набули відповідні відомості доказового значення у спосіб, передбачений КПК України. Вирішальним є не походження інформації, а набуття відповідними відомостями кримінальної процесуальної форми: отримання або збирання у порядку КПК