– суб'єкти господарювання, які здійснюють господарську діяльність, що підлягає ліцензуванню (отримання спеціального дозволу) підрозділами державного органу, де працює посадова особа.

У випадку обрання тактики пошуку (напряму) «від ознак корупційного кримінального правопорушення – до факту його вчинення» основними місцями пошуку є :

– конкретне місце дислокації органу влади та управління;

– суб'єкти господарювання, які контролюються (перевірялись) конкретною особою органу влади та управління з певними наслідками;

– органи, які здійснюють накопичення інформації про осіб, які вчинили корупційне кримінальне правопорушення (зокрема – Департамент антикорупційного законодавства та законодавства про правосуддя, який є держателем Єдиного державного реєстру осіб, які вчинили корупційне правопорушення);

– підрозділи органів влади та управління, до функцій яких віднесена робота з викривачами, кадрова робота, питання безпеки.

Деревягін Олексій Олександрович,
професор кафедри оперативно-розшукової діяльності та розкриття злочинів факультету № 2 Харківського національного університету внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

ДОСВІД ВИКОРИСТАННЯ ЕЛЕКТРОННИХ (ЦИФРОВИХ) ДОКАЗІВ ЗА РЕЗУЛЬТАТАМИ ЗДІЙСНЕННЯ РОЗШУКОВОЇ РОБОТИ В УМОВАХ ВОЄННОГО СТАНУ

Технічний прогрес є невід'ємною складовою нашого життя. Останніми роками у вітчизняній системі правових наук таких як кримінальний процес, криміналістика та оперативно-розшукова діяльність з'являється все більше досліджень, присвячених цифровізації як кримінального провадження так і оперативно-розшукової діяльності, що логічно відповідає тенденціям, умовам та обставинам розвитку нашого суспільства та необхідністю «озброювати», розвивати кримінальне процесуальне та оперативно-розшукове законодавства за вимогами часу та нагальними потребами.

Розвиток інформаційних технологій, виникнення нових галузей їх застосування та поява нових електронних пристроїв збільшили кількість видів цифрової інформації та способів її кодування й перетворення. Для перегляду й дослідження окремих видів інформації за результатами

здійснення розшукової роботи правоохоронними органами недостатньо звичайної комп'ютерної техніки зі стандартним програмним забезпеченням: для цього необхідні спеціальні електронні пристрої та спеціальне програмне забезпечення. Це спричиняє певні труднощі для слідчих, оперативних працівників, прокурорів, суддів, адвокатів, експертів та ін. Особливої актуальності проблеми використання електронних (цифрових) доказів за результатами здійснення розшукової роботи набули після відкритого повномасштабного збройного вторгнення військ рф на територію України.

Окремі слідчі (розшукові) дії, які проводяться в умовах надзвичайних правових режимів та у кримінальних провадженнях щодо кримінальних правопорушень, вчинених на тимчасово окупованих територіях мають свої особливості, пов'язані також відсутністю доступу до таких територій. Як показують результати вивчення 498 кримінальних проваджень, пов'язаних із тимчасово окупованими територіями, у 83 % проводилися огляди різноманітних інтернет-ресурсів [1, с. 297]. Значний обсяг інформації, що має значення для кримінального провадження, отримується із відкритих джерел Всесвітньої комп'ютерної мережі Інтернет, що передбачає належний порядок її отримання та в подальшому використання в якості цифрових доказів.

У судочинстві країн ЄС, США та, зокрема, в Міжнародному кримінальному суді використання цифрових доказів регулюється правовими нормами, основою яких слугують принципи роботи з цифровими доказами, викладені у Протоколі Берклі та матеріалах Наукової робочої групи з цифрових доказів (SWGDE) [2].

Протокол Берклі – практичний посібник з використання цифрової інформації з відкритим вихідним кодом при розслідуванні порушень міжнародного кримінального права, права людини та гуманітарного права, розроблений школою права Університету Каліфорнії в Берклі разом з представниками ООН. Інформація з відкритих джерел включає загальнодоступну інформацію, яку будь-який представник громадськості може спостерігати, купувати чи запитувати, не вимагаючи особливого правового статусу чи несанкціонованого доступу [3], така інформація в подальшому може бути використана в якості електронного доказу у кримінальних провадженнях.

Варто підкреслити, що в наукових колах не має чіткого визначення поняття електронних доказів. Деякі експерти розуміють цей вид доказів як «цифрові» докази. Однак з розвитком комп'ютерних технологій (цифрових технологій) він отримав назву «електронного» доказу. Науковці в галузі кримінально-правових наук одночасно використовують терміни «електронні» та «цифрові» докази, хоча ці терміни не є

тотожними. Не вдаючись до наукової полеміки відзначимо, що ми поділяємо позицію Г. Авдєєвої та Е. Живуцької-Козловської, які цифровими доказами вважають фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об'єктивного вирішення справи [4, с. 131].

На відміну від Цивільного процесуального кодексу України (ст. 100), Господарського процесуального кодексу України (ст. 96) і Кодексу адміністративного судочинства України (ст. 99), в кримінальному процесуальному законодавстві України, на жаль, взагалі відсутнє визначення терміну «цифрові докази», не визначений порядок їх збирання, зберігання, аналізу та використання у кримінальному провадженні, що значно ускладнює здійснення розшукової роботи в умовах воєнного стану. Тому судами України вони іноді не визнаються допустимими доказами [5], а напрацювання у цьому напрямі науковців і юристів ЄС та США використовуються, в основному, журналістами-розслідувачами.

За результатами узагальнення практики суду касаційної інстанції з питань проведення й оцінювання результатів НСРД у кримінальному провадженні з'ясовано, що найчастіше причинами невизнання судом допустимими доказами цифрових аудіо- та відеозаписів, здійснених під час їх проведення, є такі: надання до суду копій цифрової інформації, а не оригіналів; проведення НСРД співробітниками оперативного підрозділу без доручення на те слідчого, прокурора та без ухвали слідчого судді; невідкриття стороні захисту в порядку ст. 290 КПК доручення на проведення НСРД; відсутність процесуального оформлення рішення слідчого або прокурора про залучення до проведення НСРД «іншої особи»; невиконання вимог ч. 4 ст. 271 КПК щодо негайного складання протоколу за результатами проведення контролю за вчиненням злочину в присутності особи, щодо якої проведено НСРД, одразу після відкритого фіксування під час завершальної стадії контролю за вчиненням злочину з фактичним її затриманням [6].

Отже, підводячи певні підсумки відзначимо, що успіх здійснення розшукової роботи в умовах воєнного стану певною мірою залежить від ефективності використання електронних (цифрових) доказів у кримінальному провадженні. Під час роботи із електронними (цифровими) доказами за результатами здійснення розшукової роботи в умовах воєнного стану слідчі, співробітники оперативних підрозділів, прокурори, судді, а також судові експерти зазнають певних труднощів через швидкий розвиток і зміну технологій цифрових пристроїв та, як наслідок, – зміну технологій виявлення, вилучення, фіксації й дослідження цифрової інформації.

На сьогоднішній день виникла нагальна потреба у закріплені в Кримінальному процесуальному кодексі України норм, якими визначатимуться поняття електронних (цифрових) доказів, механізми їх отримання та використання, зокрема розмежуванням понять «електронний доказ» і «цифровий доказ»; порядок вилучення, огляду, фіксації та зберігання; порядок оцінки допустимості й достовірності тощо.

Удосконалення чинного законодавства вимагає від науковців також розробки ефективних тактичних прийомів проведення НСРД, що є актуальним і перспективним напрямом розвитку оперативно-розшукової компаративістики, з метою гармонізації національного кримінального процесуального та оперативно-розшукового законодавств у відповідності до ефективних правових приписів, виплеканих досвідом інших країн, із запровадженням яких відбулося зростання позитивного тренду у протидії кримінальним протиправностям в умовах воєнного стану.

Список використаних джерел

1. Тетерятник Г.К. Кримінальне провадження в умовах надзвичайних правових режимів: теоретико-методологічні та праксеологічні основи: монографія. Одеса: Гельветика, 2021. 500 с.

2. Positions and Considerations of Scientific Working Group on Digital Evidence. URL: https://www.swgde.org/documents/positions-and-considerations.

3. Berkeley Protocol on Digital Open Source Investigations. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_Berkeley Protocol.pdf.

4. Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. Теорія та практика судової експертизи і криміналістики. Вип. 1 (30). 2023. С. 126–143.

5. Судді Верховного Суду поділилися актуальною судовою практикою з питання доказування на підставі електронних доказів. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1155803/.

6. Узагальнення практики суду касаційної інстанції з питань проведення та оцінювання результатів НСРД у кримінальному провадженні (оновлено). *Тренінговий центр прокурорів України.* 2021. С. 51.