КРИМІНАЛЬНИЙ ПРОЦЕС, КРИМІНАЛІСТИКА, ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ, СУДОВА ЕКСПЕРТИЗА, СУДОВІ ТА ПРАВООХОРОННІ ОРГАНИ

Ковтун Л.Ю.
магістр,
курсант факультету підготовки, перепідготовки
та підвищення кваліфікації працівників податкової міліції
Науковий керівник: **Амеліна А.С.**
кандидат юридичних наук, доцент,
заступник начальника кафедри фінансових розслідувань,
Університет державної фіскальної служби України

ПРОБЛЕМНІ АСПЕКТИ ЗБИРАННЯ ТА ПЕРЕВІРКИ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

Актуальність даної теми обумовлена стрімким розвитком технологій на сьогоднішній день, що дозволяє кожній людині, не залежно від матеріального стану, вільно користуватися цим у своєму житті, наприклад обмінюватися інформацією за допомогою соціальних мереж або ж здійснювати підприємницьку діяльність в електронному режимі та інше. Однак поряд з позитивним ефектом такого явища можна також констатувати й певні негативні наслідки, такі як спрощення та полегшення процесів, пов'язаних із вчиненням кримінальних правопорушень та знищення або приховання їх слідів. Це зумовлює потребу адаптувати правову систему до кіберпростору. Прийняття Кримінального процесуального кодексу України суттєво змінило процедуру збору доказів, однак невирішеним залишилось питання збирання та перевірки електронних доказів.

Електронні докази – це сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах [1]. Джерелами електронних доказів є електронні пристрої: комп'ютери, комп'ютерні мережі, мобільні телефони, периферійні пристрої, цифрові камери та інші портативні пристрої, в тому числі мережу Інтернет [2, с. 124].

Розгляд матеріалів кримінального провадження в суді на сьогодні майже не обходиться без електронної інформації яка надається сторонами в якості доказів, наприклад роздруківки матеріалів листування із соцмережі, або іншої інформація яка зберігається в електронному вигляді.

Практика свідчить, що у значній кількості випадків під тиском представників захисту в суді електронні докази не беруться до уваги [1].

Кримінальний процесуальний закон взагалі не регулює таке явище як електронні докази – лише письмові та речові, тому суди намагаються розглядати

електронні докази в якості письмових, якщо вони залучаються на паперовому носії. Оскільки відповідальність ґрунтується на винних діях конкретної особи, то найголовніша проблема – як достовірно ідентифікувати особу, яка створила і розповсюдила певний електронний документ, що може бути доказом. Також через відсутність базового обсягу знань у галузі інформаційних технологій та повноцінно сформованої методики збирання та використання електронних доказів доводиться залучати спеціалістів, вилучати велику кількість обладнання, а також витрачати багато часу на їх пошук та фіксацію.

Таким чином консервативна традиційна система судочинства не завжди «встигає» за динамічним розвитком інформаційного суспільства й не пропонує учасникам суспільних відносин відповідних чітких та зрозумілих процесуальних інструментів, які б, з одного боку, надавали можливість учасникам судочинства повноцінно використовувати для захисту своїх прав та інтересів ті досягнення інформаційних технологій, які вони вже використовують в інших сферах суспільного життя, а з іншого боку, реально впливали на підвищення якості, ефективності та динамічності судочинства в сучасних умовах.

Змінити ситуацію на краще та забезпечити використання електронних доказів при здійсненні доказування у кримінальному процесі без необхідності проведення додаткових процесуальних дій та формування інших джерел доказів, що є досить дорогим та довготривалим процесом, можна шляхом зміни підходу до цього інституту. При цьому доцільно звернути увагу на досвід Німеччини та Франції щодо правового регулювання у вказаній сфері. Так, Німецький підхід до надання юридичної сили електронним документам на рівні із юридичною силою документів у паперовому вигляді полягає у побудуванні суворого порядку на базі регулювання використання криптографії з відкритим та закритим ключем, тобто доказова сила таких документів забезпечується наявністю електронного цифрового підпису. У Франції електронні документи отримали таке ж визнання юридичної сили, як і паперові з власноручним підписом без зв’язку із конкретним технологічним засобом [3].

Отже, узагальнюючи вищезазначене потрібно констатувати той факт, що методика збирання та перевірки електронних доказів у кримінальному процесі потребує значного вдосконалення. Враховуючи сучасні можливості криміналістики необхідно підвищити, принаймні, базовий рівень знань у галузі інформаційних технологій усіх осіб, які здійснюватимуть пошук і фіксацію та досліджуватимуть електронні докази. А також звернутися до міжнародного досвіду та надати електронним доказам такої ж самої сили, як і речовим доказам чи паперовим документам, прописуючи це саме в законодавстві не порушуючи при цьому балансу прав людини, конфіденційності, анонімності та безпеки держави і суспільства.

Список використаних джерел:

1. Котляревський О. І. Комп’ютерна інформації як речовий доказ у кримінальній справі [Електронний ресурс] / Котляревський О. І., Киценко Д. М. // Режим доступу: http://www.bezpeka.com/ru/lib/spec/crim/art70.html

2. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження / Н. М. Ахтирська. // Науковий вісник Ужгородського національного університету. – 2016. – С. 123–125.

3. Ницевич А. А. Электронный документ как доказательство [Електронний ресурс] / А. А. Ницевич – Режим доступу: http://www.rtpp.com.ua/4business/10

Куцій М.С.
викладач,
Національна академія Служби безпеки України

ЗАБЕЗПЕЧЕННЯ ПОСЕРЕДНИЦЬКОГО ЗВ'ЯЗКУ В КОНФІДЕНЦІЙНОМУ СПІВРОБІТНИЦТВІ

З метою результативного вирішення завдань оперативно-розшукової діяльності (далі – ОРД) на засадах добровільності використовується інститут конфіденційного співробітництва з різними категоріями осіб (конфіденти) [1]. Науковці вітчизняних і зарубіжних правоохоронних відомств у своїх, переважно закритих, працях досліджували питання зазначеного співробітництва та використання сучасних технологій в ОРД. Зокрема, К.В. Антонов, П.П. Артеменко, О.М. Бандурка, Б.І. Бараненко, А.Д. Безруков, М.М. Василина, В.О. Глушков, О.М. Джужа, Є.О. Дідоренко, В.Є. Марічев, С.С. Овчинський, Ю.Ю. Орлов, В.Г. Пилипчук, І.А. Серебряков, І.В. Слюсарчук, І.Ф. Хараберюш, М.О. Шилін та ін.

Але, незважаючи на проведену вказаними й іншими авторами дослідницьку роботу, спрямовану на всебічне вивчення окремих аспектів діяльності негласного апарату, комплексне дослідження процесів правового та організаційного забезпечення зв'язку у конфіденційному співробітництві з використанням сучасної техніки, представниками вітчизняної правової науки не здійснювалось, що і визначає актуальність теми. В контексті з вказаним вище необхідно, на наш погляд, приділити увагу походженню застосованої юридичної термінології, передусім термінам і поняттям, які стосуються ролі таких осіб у забезпеченні конспіративного зв'язку. Запропонований підхід дозволить уникнути термінологічних колізій серед понять, які не визначені в оперативно-розшуковому законодавстві, але широко використовуються в оперативній практиці або не відображені в юридичній науці, однак застосовуються суб'єктами нормотворчої діяльності у відповідних відомчих актах, що мають відношення до сфери конфіденційного співробітництва [2, с. 73].

Як відомо, в оперативній практиці під зв'язком оперпрацівника і конфідента (далі – виконавців завдань ОРД) розуміється їх взаємне сповіщення про необхідність зустрічі, а також конспіративне спілкування, яке надає можливість здійснювати взаємний обмін оперативно-розшуковою інформацією (далі – ОРІ) [3]. Особиста конспіративна зустріч залишається для цих виконавців основним способом їх зв'язку. Однак, при певних негативних умовах, проведення таких зустрічей неможливо внаслідок загроз особистій