

принципу змагальності сторін у досудовій стадії кримінального провадження. Тому віднесення потерпілого, його законного представника та представника, а також цивільного позивача і його представника сприяло б ефективності судового розгляду.

Список використаних джерел

1. Конвенція про захист прав людини і основоположних свобод (Рим, 4.XI.1950) // *Голос України*. – 2001. – № 3. – 10 січня. – С. 6-8.
2. Кримінальний процесуальний кодекс України від 05.04.2001 р. № 2341-III // *Відомості Верховної Ради України*. – 2001. – № 25/26. – Ст. 131.
3. Зінченко О.В. Змагальність у досудовому розслідуванні: сутність та суб'єктний склад сторони обвинувачення / О.В. Зінченко // *Вісник Харківського національного університету*. – 2017. – № 23. – С. 181-183.
4. Мірошников І.Ю. Реалізація принципу змагальності на судовому слідстві в апеляційному суді / І.Ю. Мірошников // *Вісник прокуратури*. – 2003. – № 8. – С. 62-64.

Науковий керівник: к.ю.н., доцент Мудрак І. В.

Шишацька Юлія Олегівна

студентка 1-го курсу магістратури факультету прокуратури
та слідства (кримінальної юстиції)

Національного університету «Одеська юридична академія»

РОЗВИТОК КРИМІНАЛЬНОГО ПРОЦЕСУАЛЬНОГО ЗАКОНОДАВСТВА УКРАЇНИ ЩОДО ЕЛЕКТРОННИХ ДОКАЗІВ В СУЧАСНОМУ КІБЕРПРОСТОРІ

Варто визнати, що сьогодні ми існуємо у цифрову еру, яка з кожним днем все більше видозмінює усталені засоби створення, відображення, передачі, знищення, а також використання інформації. Проте, необізнаність населення у сфері ІТ-технологій стає сприятливим середовищем для противоправних дій кіберзлочинців. Однак сучасне законодавство не пристосоване до кіберпростору, а

тому і залишилось питання щодо невизнання місця регламентації електронних доказів у процесуальному законодавстві.

Відповідно до глави 4, ст. 84 Кримінального процесуального кодексу України доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку [1].

Прийняття Кримінального процесуального кодексу України суттєво змінило процедуру збирання доказів, однак не вирішеним залишилось питання належної правової процедури збирання, зокрема, належної фіксації, електронних доказів. Йдеться, зокрема, про визначення електронних доказів, способи їх одержання, визначення їх належності, допустимості, можливості використання міжнародної правової допомоги в розкритті IP-адрес користувачів світової мережі у випадку підозри щодо вчинення ними кримінальних правопорушень тощо [2, с. 123].

Більш того, через несучасність та невідповідність часові кримінально-процесуальних норм, сьогодні ми продовжуємо використовувати тлумачення законодавців в Цивільному процесуальному кодексі України щодо електронних доказів.

Варто зазначити, що розробці концепції кібердоказів у вітчизняній науці кримінального процесу та криміналістики було недостатньо приділено уваги. Одною із таких причин можна вважати як брак технічної освіти та знань в IT-сфері у правознавців. Неможливо розробляти механізм протидії кіберзлочинам, якщо не розуміти як діятимуть потенціальні злочинці і як їх можна зупинити.

Із цього виходить, що саме невизначеність електронних доказів в законодавстві нашої країни призводить до загрози інформаційній безпеці наших громадян та робить нас вразливими до особливої групи кримінальних правопорушень – кіберзлочинів.

З огляду на вищезазначене, на законодавчому рівні пропонується закріпити, що електронні докази – це дані, які підтверджують факти, інформацію або концепцію у формі, придатній для обробки за допомогою комп'ютерних систем, у тому числі програми виконання комп'ютерною системою або інших дій. Джерелами електронних доказів доцільно визнавати електронні пристрої: комп'ютери, периферійні пристрої, комп'ютерні мережі, мобільні телефони, цифрові камери та інші портативні пристрої, в тому числі мережу Інтернет. Інформація з цих джерел не має фізичної форми [2, с. 125]. Проте, доцільним було б врахування у визначенні електронних

доказів того, що відповідні дані мають встановлювати наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Крім того, відповідна інформація, дійсно, не має фізичної форми, проте, вона має бути вилучена і оформлена у встановленому КПК України порядку, який теж потребує розробки та закріплення у чинному кримінальному процесуальному законодавстві, для того, щоб ці дані мали властивість допустимості.

В умовах ІТ-глобалізації позитивно впливає на національне правотворення, досвід країн Європейського союзу та США, де за допомогою прецедентного права визначають процес збору доказів (зокрема, електронних). Саме це може слугуватиме прикладом, в якомусь розумінні, і стимулом до змін у кримінальному процесуальному законодавстві України, та у майбутньому стати міцним фундаментом у захисті наших громадян проти кіберзлочинів.

Список використаних джерел

1. Кримінальний процесуальний кодекс України від 13 квітня 2012 року (із змінами та доповненнями) // Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст. 88. [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/4651-17>
2. Ахтирська Н.М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження, Науковий вісник Ужгородського національного університету, 2016 [Електронний ресурс]. – Режим доступу: http://www.visnyk-juris.uzhnu.uz.ua/file/No.36/part_2/32.pdf

Науковий керівник: д.ю.н., доцент Гловюк І. В.