ІМПЛЕМЕНТАЦІЇ ОКРЕМИХ НОРМ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ У ВІТЧИЗНЯНЕ ЗАКОНОДАВСТВО, ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Бердиченко І.О., начальник відділу аналітичного забезпечення Департаменту кіберполіції Національної поліції України, кандидат юридичних наук.

Основою для здійснення заходів у боротьбі з кіберзлочинністю є ефективне законодавство, що відповідає вимогам із забезпечення дотримання прав людини і верховенства закону. Це особливо стосується конкретних повноважень в межах кримінального процесуального законодавства, що передбачені в Конвенції про кіберзлочинність (ратифікована Україною із застереженнями і заявами Законом N 2824-IV від 07.09.2005), як всеосяжній основі вітчизняного законодавства для таких повноважень, а також сприяє міжнародному співробітництву у боротьбі з кіберзлочинністю.

В Преамбулі Конвенції про кіберзлочинність (далі – Конвенція), серед іншого, наголошено на першочерговій необхідності спільної політики, спрямованої на захист суспільства від кіберзлочинності, між іншим, шляхом створення відповідного законодавства.

Проголошено про глибокі зміни, спричинені переходом на цифрові технології, конвергенцією і глобалізацією комп'ютерних мереж, яка продовжується, стурбованість ризиком того, що комп'ютерні мережі та електронна інформація може також використовуватися для здійснення кримінальних правопорушень, і того, що докази, пов'язані з такими правопорушеннями, можуть зберігатися і передаватися такими мережами.

Стратегічним пріоритетом вважається прийняття ефективного законодавства у сфері боротьби з кіберзлочинністю та застосування електронних доказів, яке б відповідало вимогам із забезпечення дотримання прав людини і верховенства закону.

Унаслідок аналізу вітчизняного законодавства та порівняння його положень із нормами Конвенції про кіберзлочинність встановлено ряд напрямків, які потребують опрацювання.

Ці питання перш за все, стосуються необхідності імплементувати у вітчизняне законодавство запобіжні заходи, визначенні Конвенцією, зокрема визначені у ст. 16 (Термінове збереження комп'ютерних даних, які зберігаються) та 17 (Термінове збереження і часткове розкриття даних про рух інформації).

Вирішення цих питань, як зазначено у Конвенції, буде сприяти підвищенню ефективності кримінальних розслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину, в електронній формі.

Наразі у вітчизняному законодавстві відсутнє визначення терміну «електронні докази». Конвенція не містить визначення поняття «електронних доказів». Проте для того щоб імплементувати статті Конвенції, які стосуються процесуальних заходів, варто було б визначити таке явище. Ситуацію можна виправити шляхом запровадження до Кримінального процесуального кодексу спеціальної дефініції поняття «цифрових (електронних) доказів».

Тому пропонується доповнення Кримінального процесуального кодексу України статтею 99-1 (Цифрові докази) наступного змісту:

1. Цифровим доказом є інформація, що зберігається або передається у цифровій (електронній) формі, отримана у передбаченому цим Кодексом порядку, на підставі якої слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

2. Цифрові докази отримані шляхом копіювання (відтворення) та/чи збереження інформації у цифровій (електронній) формі за правилами, встановленими цим Кодексом, визнаються допустимими доказами у кримінальному провадженні.

3. Цифрові (електронні) докази можуть бути у формі речових доказів та документів».

Для реалізації положень ст. 16,17 Конвенції є доцільним передбачити у Кримінальному процесуальному кодексі окремі правові норми щодо запровадження термінової фіксації інформації в цифровій (електронній) формі, як заходу забезпечення кримінального провадження.

На наш погляд, термінова фіксація інформації в цифровій (електронній) формі полягає у невідкладному фіксуванні та подальшому зберіганні комп'ютерних даних із забезпеченням їх цілісності та неспростовності, у тому числі даних про трафік, операторами та провайдерами телекомунікацій на носії інформації.

Термінова фіксація інформації в цифровій (електронній) формі повинна здійснюватися на підставі ухвали слідчого судді.

Строк термінової фіксації інформації в цифровій (електронній) формі та/або тимчасового обмеження (блокування) доступу довизначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу), адреси мережі Інтернет, домену, не може перевищувати 90 днів, з можливістю подальшого продовження слідчим суддею в межах строку досудового розслідування.

Разом з тим, у практичній діяльності правоохоронних органів викникають випадки, коли існує необхідність у терміновій фіксації інформації в цифровій (електронній) формі до постановлення ухвали слідчого судді, за постановою прокурора або постановою слідчого, погодженою прокурором. Такі випадки, перш за все, можуть виникнути при необхідності врятування життя людей та запобігання вчиненню тяжчого чи особливо тяжкого кримінального правопорушення. На наш погляд строк 48 годин є достанім для звернення прокурора, слідчого за погодженням з прокурором до слідчого судді для отримання дозволу на проведення термінової фіксації інформації.У разі відмови слідчого судді в наданні дозволу на проведення цих дій або після закінчення строку, на який було здійснено термінову фіксацію інформації в цифровій

(електронній) формі отримана інформація визнається недопустимою як докази та підлягає знищенню.

Таким чином, запровадження дефініції для електронних доказів, значно спростило б процес розробки конкретних процесуальних заходів для імплементації окремих положень Конвенції у вітчизняне законодавство. По- друге, запровадження поняття «цифрових (електронних) доказів» збільшить правову чіткість і передбачуваність закону, а імплементації правових норм Конвенції буде сприяти приведенню відчизняного законодавства у відповідність до норм Європейського законодавства, у частині процедури збору та використання таких доказів.

Список використаних джерел

1. Конвеція про кіберзлочинність [Електронний ресурс].– Режим доступу: http://zakon2.rada.gov.ua.

2. Кримінальний процесуальний кодекс України [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua.