Список використаних джерел

1. Конституція України: прийнята на п'ятій сесії Верховної Ради України від 26 червня 1996 року від 01.10.2010 – 2010 р. / № 72/1 Спеціальний випуск, стор. 15, стаття 2598.
2. Кримінальний процесуальний кодекс України: Закон України від 25.05.2012 – 2012 р., № 37, стор. 11, стаття 1370, код акта 61601/2012
3. Кодекс професійної етики та поведінки прокурорів, затверджений 27 квітня 2017 року № 1387-IV // ВВР. – 2017 – № 4-5. – Ст. 121.

Ключові слова: державне обвинувачення, прокурор, межі судового розгляду, приватне обвинувачення, відносини прокурора з іншими учасниками кримінального провадження.

Науковий керівник: к.ю.н., доцент Шилін Д.В.

Шишацька Юлія Олегівна

студентка 4-го курсу Інституту кримінальної юстиції
Національного університету «Одеська юридична академія»

ВИЯВЛЕННЯ ДОКАЗІВ КІБЕРЗЛОЧИНУ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Сучасний прогресивний розвиток інформаційних технологій, призводить до зростання ролі мережевих технологій у житті кожної людини, і, як наслідок, значна частина соціальних комунікацій, економічних інституцій тощо переміщується у віртуальне середовище – кіберпростір, тобто інтерактивне інформаційне середовище, яке функціонує на базі електронних інформаційних систем. Сьогодні, усі сфери суспільного життя активно включенні у інтернет-простів, зокрема: банкінг, інтернет-магазини, онлайн консультації фахівців, служба доставки, соціальні мережі спілкування і знайомств та інше. Пропорційно до зростання рівня інтересу та популяризації Веб-ресурсів, зростає та розвивається злочинність у цій сфері. З'являються так звані «кіберзлочини» – передбачене кримінальним законом суспільно небезпечне винне діяння, що полягає в протиправному використанні інформаційних та комунікативних технологій, відповідальність за яке встановлена законодавством про кримінальну відповідальність [2, с. 434].

Враховуючи значні обсяги інформації, які циркулюють у мережі Інтернет, її цінності для вирішення завдань протидії злочинності та досудового розслідування злочинів, безперечної актуальності набуває проблематики вироблення уніфікованих моделей та методик виявлення

та фіксації цифрової інформації для подальшого її використання у доказуванні, на що звертають увагу й інші дослідники [4].

Безумовно, для працівників правоохоронних органів та правозахисників, означена проблематика не є новою, зокрема усталеним у юридичній практиці відповідний понятійно-категоріальний апарат, який використовується на рівні контрактів, а подекуди і у законодавстві. Водночас, відсутність чіткої моделі правового регулювання мережі Інтернет, а також безапеляційних методик виявлення та фіксації цифрової інформації, створює нові юридичні проблеми процесуального характеру щодо виявлення комп'ютерних злочинів, вилучення даних з інформаційних систем та електронно-обчислювальних машин, кваліфікація діянь і доказування такої злочинної діяльності.

Саме тому слідом за розвитком електронних інформаційних систем та девайсів, також повинна розвиватись і правоохоронна діяльність. Усвідомлюючи особливість «інтерактивних» злочинів, в Україні були реформовані підрозділи боротьби з кіберзлочинністю МВС в Департамент кіберполіції Національної поліції України [3]. Такі позитивні кроки для боротьби з особливою групою злочинів є очікуваними, проте вивчення практики роботи таких підрозділів свідчить про недостатність у працівників необхідного досвіду та навичок, а також недосконале структурування, відсутність розмежування компетенції підрозділів Департаменту, неясність у нормативно-правовій базі, відсутність методик розслідування кіберзлочинів, що створює значні проблеми під час розкриття кримінальних правопорушень, які вчиненні із використанням високих інформаційних технологій.

Також акцентуємо увагу на одну із найголовніших проблем – виявлення доказів кіберзлочинів. Майже усі кіберзлочини являються діяннями із високою латентністю. Іноді можна дізнатись про злочин у визначений час або коли вже настануть незворотні кримінальні наслідки. Тому питання визначення місця злочину та використання девайсів – знаряддя злочину, як ніколи актуальне. У деяких випадках такі злочини мають транснаціональний характер, а саме: кіберзлочин вчинений за кордоном, об'єктом якого є інформація вилучена із комп'ютера в Україні.

Крім цього, якщо спеціалісти в сфері IT-технологій виявили злочинця та встановили IP-адресу (англ. Internet Protokol address – ідентифікатор мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах [2, с. 427], тоді можливо тимчасово вилучити електронну інформаційну систему або електронно-обчислювальну машину під час обшуку. Відповідно до ст. 234 ч. 2 Кримінального процесуального кодексу України (далі – КПК України) обшук проводиться на підставі ухвали слідчого судді. Важливо зазначити, що за цей час, поки буде отримана ухвала слідчого судді, є можливість знищити усю інформацію, що є фактом вчинення противоправного діяння. Тому потрібне уточнення щодо процесуаль-

них дій відносно кібернетичних засобів збереження інформації у кримінальному провадженні, а саме розширення можливості проведення знаття інформації з електронних інформаційних систем не лише у кримінальних провадженнях стосовно тяжких та особливо тяжких злочинів, зокрема, у випадках, коли доступ до електронних інформаційних систем чи їх частин обмежується її власником, володільцем або утримувачем або пов'язаний з подоланням системи логічного захисту. Таким чином, буде забезпечен збереження необхідних для розслідування фактичних даних.

Друге питання, що є досить відкритим сьогодні – це строки тимчасового вилучення майна. Відповідно до розділу 16 КПК України тимчасового вилучення майна, а саме вилучення електронно-обчислювальних машин (комп'ютерів) чи пристроїв не має чітких визначених часових меж для повернення володільцям. Практика показує, що технічні засоби можуть бути вилучені, поки триває досудове розслідування.

З огляду на вищезазначене, подальший процес реформування кримінального процесуального законодавства України повинен здійснюватися з урахуванням інноваційного розвитку інформаційних технічних засобів використання Інтернет-простору. Тільки у таких умовах можлива продуктивна діяльність правоохоронних органів в рамках кримінального провадження щодо 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. ІТ-право: теорія та практика : навч. посіб. / авт. кол. ; за ред. Є.О.Харитонова, О.І. Харитонової. – Одеса : Фенікс, 2017. – 472 с.
3. Департамент кіберполіції Національної поліції України [Електронний ресурс]. – Режим доступу: https://www.npu.gov.ua/uk/publish/article/1816252
4. Малахова О.В. До питання огляду сторонами кримінального провадження змісту інтернет-сторінок: Вісник кримінального судочинства. – 2017. – № 2. – С. 64-69. [Електронний ресурс]. – Режим доступу: http://vkslaw.knu.ua/images/verstka/2_2017_Malahova.pdf

Ключові слова: кіберзлочинність, кіберзлочин, обшук.

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