ЮРТАЄВА Ксенія
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і кримінології факультету № 1
Харківського національного університету внутрішніх справ,
м. Харків, Україна

УДОСКОНАЛЕННЯ ПІДГОТОВКИ ТА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ СУДДІВ ЩОДО СУДОВОГО РОЗГЛЯДУ СПРАВ ПРО ЗЛОЧИНИ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Реформа судової системи є пріоритетним напрямом у практичній реалізації вектору європейської інтеграції України та побудови дієвої системи влади в складних соціально-політичних умовах сьогодення. Особливостями реалізації реформи судової системи в Україні є те, що вона проходить паралельно з реформою правоохоронних органів, й потребує масштабної підготовки нових кваліфікованих суддівських кадрів, здійснення перепідготовки судів із врахуванням сучасних напрямів розвитку правової системи нашої держави і загальносвітових тенденцій. Особливо актуальним у цьому зв'язку стає напрям вдосконалення професійних знань суддів щодо судового розгляду злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та кіберзлочинів загалом. При цьому слід наголосити, що поняття кіберзлочинів наразі є більш широким за поняття злочинів, передбачених у розділі XVI Особливої частини Кримінального кодексу (далі – КК України) (ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»), і саме кіберзлочини як новий вид транскордонної злочинності мають низку особливостей щодо кваліфікації та судового розгляду. Відповідно вбачається, що кіберзлочинність як новий правовий феномен вимагає посиленої уваги під час підготовки та перепідготовки суддівських кадрів.

Важливість зазначеного напряму підкреслюється тим фактом, що кібербезпека визнана важливою складовою національної безпеки України поряд з воєнною та громадською безпекою держави (ст. 1, 3 Закону України «Про національну безпеку України»). Необхідність вдосконалення підготовки суддів (слідчих суддів), слідчих та прокурорів щодо роботи з доказами, що стосуються злочинів, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів також визначена в п. 4.5 Стратегії кібербезпеки України. Не-

зважаючи на зазначені стратегічні завдання національного значення статистика Генеральної Прокуратури України продовжує демонструвати низький рівень розкриття та досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: у 2016 році було зареєстровано 865 кримінальних правопорушень цього виду і лише 405 були направлені до суду з обвинувальним актом, у 2017 році було зареєстровано 2573 кримінальні правопорушення і 1015 були направлені до суду з обвинувальним актом, у 2018 році було зареєстровано 2301 кримінальне правопорушення і 1330 були направлені до суду з обвинувальним актом [1]. Звісно, такі статистичні дані не здатні повною мірою продемонструвати справжню динаміку кіберзлочинності в Україні, адже зазначений вид злочинів характеризуються надлатентністю [2], або кіберлатентністю, тобто їх реальна кількість в 100 і більше разів перевищує офіційні статистичні показники. Наявна ж судова статика взагалі надає наднизькі показники щодо розгляду цієї категорії справ [3]. Причинами такої ситуації, зокрема, можна визначити труднощі у виявленні фактів вчинення кіберзлочинів, недосконаліть кримінально-процесуальних норм, щодо фіксації та використання електронних доказів під час проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та судового розгляду, недоліки щодо експертних методик дослідження електронних доказів, які часто не встигають за сучасним розвитком комп'ютерних технологій, а також низький рівень правових знань працівників правоохоронних та судових органів щодо розслідування та судового розгляду кіберзлочинів. Зазначені фактори помножуються на той факт, що кіберзлочини, які в переважній більшості вчиняються з використанням міжнародних комп'ютерних мереж, зокрема Інтернет, мають транскордонний характер, а суди в Україні вкрай неохоче використовують кримінальну юрисдикцію позатериторіально, незважаючи на те, що така можливість передбачена в КК України і подібна практика є доволі розповсюдженою в зарубіжних країнах (див., наприклад, матеріали справи щодо А. Вауліна [4]).

Аналіз судової практики щодо розгляду злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також інших кібезлочинів, передбачених у КК України, виявляє, що суди не завжди правильно здійснюють кваліфікацію кіберзлочинів, зокрема відмежування злочину, передбаченого у ч. 3 ст. 190 КК України, від злочинів передбачених у ст.ст. 185 і 191 КК України [5], що призводить до необхідності виправлення зазначених помилок в апеляційному порядку [6]. Наразі Верховний суд України не прийняв жодних рекомендацій у вигляді постанови або правої позиції щодо кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що ставить суди першої та апеляційної інстанцій перед необхідністю самостійного тлумачення зазначених норм, що часто призводить не лише до відмінного їх застосування, а й до

помилок в кваліфікації цих діянь. Звісно, не останнє місце при цьому відіграє недосконаліть самого законодавства щодо закріплення кримінальної відповідальності за кіберзлочини, що є предметом наукових дискусій [7; 8].

Резюмуючи, слід підкреслити, що підвищення якості підготовки та підвищення кваліфікації суддів і працівників правоохоронних органів є необхідною умовою вдосконалення протидії злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Як один з розробників та тренерів курсу програми спеціальної підготовки кандидатів на посаду судді Національної школи суддів України «Особливості здійснення судового розгляду щодо злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Кібербезпека та права людини в мережі Інтернет», вважаю доцільним продовжувати позитивну практику використання новітніх інтерактивних методик викладання (мінілекція, опитування з використання клікерів, мозковий штурм, вирішення практичних завдань, робота у малих групах тощо), що активно запроваджуються в навчальний процес Національної школи суддів України та позитивно впливають на засвоєння навчального матеріалу слухачами, а також: продовжувати вдосконалення практичних завдань з кваліфікації кібезлочинів з врахуванням сучасної судово-слідчої практики з метою уніфікації судового розгляду справ цієї категорії; розробити рекомендації щодо особливостей застосування кримінальної юрисдикції щодо кіберзлочинів (в тому числі й позатериторіально) та впровадити їх навчальних процес підготовки та підвищення кваліфікації суддів; розробити та впровадити навчальних процес рекомендації щодо дослідження електронних доказів у судовому засіданні.

Список використаних джерел:

1. Єдиний звіт про кримінальні правопорушення за 2016, 2017, 2018 роки. URL: https://www.gp.gov.ua/ua/stst2011.html (дата звернення: 10.08.2019).

2. Орлов О.В. Організаційні та нормативно-правові засади боротьби з кіберзлочинністю. *Державне управління: удосконалення та розвиток.* № 5. 2014. URL: http://www.dy.nayka.com.ua/?op=1&z=715 (дата звернення: 10.08.2019).

3. Звіт судів першої інстанції про розгляд справ у порядку кримінального судочинства (2017). URL: https://court.gov.ua/inshe/sudova_statystyka/ rik_2017 (дата звернення: 10.08.2019).

4. В Польше арестован харьковчанин, владеющий крупнейшим мировым торрент-трекером. URL: https://ain.ua/2016/07/21/arestovan-ukrainec-vladelec-krupnejshego-torrenta-ego-obvinyayut-v-piratsve-na-1-mlrd/ (дата звернення: 10.08.2019).

5. Вирок Вишгородського районного суду Київської області від 12.10.2017, справа № 363/2491/17. URL: http://reyestr.court.gov.ua (дата звернення: 10.08.2019).

6. Вирок Колегії суддів судової палати з розгляду кримінальних справ апеляційного суду Хмельницького області від 20.05.2015, справа № 686/26351/14-к. URL: http://reyestr.court.gov.ua/Review/44283337 (дата звернення: 10.08.2019).

7. Васильєв А.А., Пашнєв Д.В. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Вісник Кримінологічної асоціації України*. 2013. № 5. С. 34–42.

8. Юртаєва К.В. Проблеми криміналізації незаконного використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин. *Форум права.* 2017. № 3. С. 221–227.