окреслені законом, а її реалізація супроводжуватись ефективними гарантіями судового контролю. Саме відсутність таких гарантій часто стає підставою для констатації порушення Конвенції. Таким чином, у сучасному розумінні ЄСПЛ правова визначеність фактично виконує функцію механізму стримування державного свавілля.

Загалом аналіз практики ЄСПЛ [11] дозволяє сформулювати декілька узагальнюючих висновків, а саме те, що принцип правової визначеності у практиці Суду трансформувався з допоміжного елементу верховенства права у самостійний універсальний стандарт оцінки якості державного регулювання. Сучасний підхід ЄСПЛ орієнтований не лише на формальну чіткість правових норм, а насамперед на забезпечення реальної передбачуваності поведінки держави для особи. Суд пов'язує правову визначеність із довірою до держави, стабільністю правового порядку та ефективністю судового захисту. Практика ЄСПЛ демонструє тенденцію до посилення вимог щодо передбачуваності законодавства у сферах, які безпосередньо стосуються демократії, політичної конкуренції та фундаментальних прав людини. Зрештою, правова визначеність у розумінні Суду є динамічною категорією, яка охоплює не лише законодавство, а й адміністративну практику, судове тлумачення, виконання рішень судів та загальну послідовність державної політики.

Важливим є і те, що практика ЄСПЛ формує модель правової визначеності, за якої ключове значення має не формальне існування правової норми, а її здатність реально гарантувати особі захист від непередбачуваного та свавільного втручання держави. Саме тому правова визначеність у сучасній практиці Суду постає не лише техніко-юридичною характеристикою права, а фундаментальною гарантією свободи людини у демократичному суспільстві.

Список використаних джерел

1. Sunday Times v. the United Kingdom (No. 1), application no. 6538/74, judgment of 26 April 1979. *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng?i=001-57584

2. Rekvényi v. Hungary, application no. 25390/94, judgment of 20 May 1999. *European Court of Human Rights*. URL: https://hudoc.echr.coe.int/eng?i=001-58262

3. Vyerentsov v. Ukraine, application no. 20372/11, judgment of 11 April 2013. *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng?i=001-118393

4. Magyar Kétfarkú Kutya Párt v. Hungary, application no. 201/17, judgment of 20 January 2020. *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng?i=001-200384

5. Centro Europa 7 S.R.L. and Di Stefano v. Italy, application no. 38433/09, judgment of 7 June 2012. *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng?i=001-111399

6. Bežanić and Baškarad v. Croatia, applications nos. 16140/15 and 13322/16, judgment of 19 May 2022. *European Court of Human Rights*. URL: https://hudoc.echr.coe.int/eng?i=001-217218

7. Brumărescu v. Romania, application no. 28342/95, judgment of 28 October 1999. *European Court of Human Rights*. URL: https://hudoc.echr.coe.int/eng?i=001-58337

8. Nejdet Şahin and Perihan Şahin v. Turkey, application no. 13279/05, judgment of 20 October 2011. *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng?i=001-107156

9. Kokkinakis v. Greece, application no. 14307/88, judgment of 25 May 1993. *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng?i=001-57827

10. Del Río Prada v. Spain, application no. 42750/09, judgment of 21 October 2013. *European Court of Human Rights*. URL: https://hudoc.echr.coe.int/eng?i=001-127697

11. Огляд практики Європейського суду з прав людини щодо застосування принципу юридичної визначеності: окремі аспекти. *Офіс Ради Європи в Україні*. URL: https://rm.coe.int/17-10-web-overview-of-the-practice-of-the-european-court-of-human-righ/1680ad380c

Сербин Руслан Андрійович, *ректор НАВС, доктор юридичних наук, професор*

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПРАВООХОРОННИХ ОРГАНІВ У ПРОТИДІЇ КІБЕРЗАГРОЗАМ

Розуміння безпеки як суспільного блага та перехід її загроз від державних до недержавних означає, що країни повинні дедалі активніше займатися діяльністю за межами власних кордонів. Загальновизнаною та однією з найкритичніших загроз глобальній стабільності є кіберзагроза, яка не обмежується крадіжкою даних, а охоплює масштабні атаки, що паралізують критичну інфраструктуру, дестабілізують економіку та втручаються в геополітичні процеси. Отже, кіберзагрози передбачають широкий спектр діяльності – від шкідливого програмного забезпечення до атак соціальної інженерії, становлять значний виклик цифровій безпеці.

Складність боротьби з кіберзлочинністю полягає не лише в темпах її зростання, а й у тому, що вона майже завжди є транскордонним явищем, коли злочинці спрямовують увагу на жертв в іноземних країнах, щоб знизити ризик переслідування. Транскордонні атаки ускладнюють боротьбу з кіберзлочинністю для правоохоронних органів, які обмежені національними кордонами. Проблему, слушно зауважує керівник ініціативи «Атлас кіберзлочинності» Шон Дойл, посилює те, що чимало країн лише починають розбудовувати потенціал своїх поліцейських сил для боротьби з кіберзлочинністю [1].

У боротьбі з кіберзлочинністю, яка вимагає швидкої оперативної співпраці та дій, міжнародна співпраця неминуча. У контексті транскордонного характеру кіберзагроз співпраця правоохоронних органів різних держав стає визначальним чинником успішної боротьби з глобальною кіберзлочинністю. Така взаємодія реалізується через механізми оперативного обміну даними, проведення спільних слідчих дій, а також взаємне надання експертно-технічної підтримки тощо.

Визнаючи міжнародний характер кіберзлочинності, українські правові механізми забезпечують ефективну співпрацю з міжнародними правоохоронними органами, розвідувальними службами та судовими системами. Однак усі ці механізми міжнародної співпраці не мають особливої цінності, якщо країни не мають можливості моніторити й аналізувати кіберпростір, а також можливості реагувати на інциденти. Тому основними темами майже кожного міжнародного кіберфоруму є моделі різних країн щодо організації системи кібербезпеки та захисту критичної інформаційної інфраструктури. Отже, глобальна кібербезпека настільки сильна, наскільки сильна її найслабша ланка.

Загальновідомо, що першим міжнародним договором, що стосується кіберзлочинності, є Будапештська конвенція від 23 листопада 2001 року, яка свого часу заохотила співпрацю між державами в розслідуванні кіберзлочинів, передусім тих, що мають транскордонні елементи. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності 2000 року, хоча й ширша за сферою застосування, також розглядає кіберзлочинність як частину глобальних зусиль щодо запобігання злочинності. Як і Будапештської, її впровадження гальмують повільні темпи міжнародної співпраці, передусім щодо доступу до цифрових доказів. Ця проблема ускладнюється залежністю від договорів про взаємну правову допомогу, які є громіздкими й неефективними у випадках, що вимагають швидкого доступу до нестабільних даних.

Регіональні рамки, такі як Міжамериканська конвенція про кіберзлочинність 1999 року та Конвенція Африканського Союзу про кібербезпеку та захист персональних даних 2014 року, спрямовані на боротьбу з кіберзлочинністю в межах певних географічних регіонів, проте вони постають перед схожими викликами.

Неузгоджені правові стандарти в різних країнах призводять до складнощів у забезпеченні дотримання законів, натомість брак широкого впровадження ще більше фрагментує глобальні зусилля щодо ефективного подолання проблеми.

Хоча співпраця між різними країнами в боротьбі з кіберзлочинністю має численні переваги, вона не позбавлена викликів і проблем, які можуть вплинути на її ефективність. Одним з головних викликів міжнародної співпраці в боротьбі зі злочинністю є необхідність координації зусиль між різними країнами. Правові обмеження, культурні відмінності та мовні бар'єри можуть створювати значні перешкоди для ефективної співпраці. Основними проблемами, що постають під час такої співпраці, є різні підходи до конфіденційності (США мають ліберальніший підхід до моніторингу даних заради національної безпеки, що викликає занепокоєння в країнах ЄС), несформованість єдиних процедур, спрощених механізмів тощо.

Оскільки кіберзлочини можуть бути вчинені навіть тоді, коли злочинці й цільові жертви не перебувають в одному місці, важливо, щоб країни розробили скоординовану систему співпраці. Однак регіональні відмінності в законодавстві можуть створювати перешкоду для боротьби з кіберзлочинністю. Контент, який вважають незаконним в одній країні, може бути легально відображений на сервері в іншій. Більшість видів взаємної правової допомоги ґрунтується на подвійній злочинності, що означає, що розслідування охоплюють кримінальні діяння в усіх постраждалих країнах, що призводить до проблем, коли закони не узгоджуються. Тому запобігання створенню безпечних притулків для злочинців є ключовим завданням у запобіганні кіберзлочинності. Адже наявність таких безпечних притулків надає можливість правопорушникам продовжувати свою протиправну діяльність і перешкоджати розслідуванню [2].

9 серпня 2024 року Генеральна Асамблея Організації Об'єднаних Націй ухвалила Конвенцію про кіберзлочинність, текст якої її прихильники вважають важливим кроком до створення універсальної правової бази для боротьби із сучасними кіберзагрозами. Ці загрози охоплюють не лише злом конфіденційних даних, а й такі дії, як атаки програм-вимагачів, онлайн-шахрайство та вторгнення в критичну інфраструктуру, які мають міжнародні наслідки [3]. Прийняття аналізованої Конвенції спричинило різку критику, зокрема з боку захисників цифрових прав. Чимало країн Заходу (включаючи Україну) висловлювали побоювання, що Конвенцію ООН можна використовувати для розширення державного нагляду або обмеження свободи слова, а також що вона містить недостатньо жорсткі механізми захисту прав людини.

Водночас Конвенція має і прогресивні положення, що виявляються передусім у зміцненні міжнародної співпраці, спрощенні доступу до даних для завдань розслідування та створенні ефективніших судових механізмів для боротьби з транснаціональною кіберзлочинністю. Це сприятиме подоланню унікальних проблем, що виникають через кіберзлочинність. Одним з головних завдань Конвенції Організації Об'єднаних Націй про кіберзлочинність є створення раціональної та ефективної міжнародної системи співпраці між державами з метою ефективної боротьби з кіберзлочинністю. До прийняття цієї Конвенції механізми міжнародної співпраці часто були фрагментованими, кожна держава мала власні процедури, що ускладнювало транскордонні розслідування та кримінальне переслідування. Тому

Конвенція встановила спільну та скоординовану правову базу для подолання цих перешкод і підвищення ефективності боротьби із цифровою злочинністю.

Позитивно оцінюємо приписи ст. 35 Конвенції [4], яка конкретно встановлює низку загальних принципів, що стосуються міжнародного співробітництва, спрямованих на сприяння розслідуванню та переслідуванню кіберзлочинів. Ця норма передбачає, що держави-учасниці мають співпрацювати відповідно до положень Конвенції та інших міжнародних документів про кримінальне співробітництво. Метою є забезпечення взаємної допомоги в збиранні, отриманні, збереженні та розкритті електронних доказів, зокрема щодо кіберзлочинів, а також інших серйозних правопорушень з міжнародним виміром. Така співпраця поширюється на заморожування, вилучення, конфіскацію та повернення доходів від злочинної діяльності, підвищуючи ефективність переслідування та виключаючи безкарність кіберзлочинців.

Привертають увагу й положення ст. 35 аналізованого міжнародного документа [4], відповідно до якої встановлено імперативне правило щодо спрощення процедур надання правової допомоги. Визначений механізм надає можливість компетентним органам держав-учасниць оперативно взаємодіяти під час розслідування широкого кола злочинів, включаючи несанкціоноване втручання в роботу комп'ютерних систем, кібершахрайство, кібербулінг і правопорушення у сфері обробки персональних даних. Слід зауважити, що нормативно закріплено принцип гнучкості співробітництва, згідно з яким вимога подвійної криміналізації не є абсолютною перешкодою. Тобто навіть за відсутності ідентичної кваліфікації діяння в національних законодавствах обох держав правова допомога може бути надана за умови, що це діяння є кримінально караним в обох країнах, і це суттєво розширює можливості міжнародного співробітництва.

З огляду на викладене, переконані, що ухвалення нової Конвенції ООН про кіберзлочинність створює належну базу для міжнародної співпраці в цифровій сфері. Однак ефективність цієї системи залежить від того, наскільки послідовно буде дотримано баланс між забезпеченням безпеки та захистом прав людини. Такий підхід потребує злагоджених зусиль, постійної пильності та високого рівня відповідальності всіх суб'єктів міжнародних правовідносин.

Список використаних джерел

1. Sean Doyle. Cybercrime and violent crime are converging: here's how to deal with it. *World economic forum*. 2023. URL: https://www.weforum.org/stories/2023/10/cybercrime-violent-crime/

2. Douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale Salvador (Brésil), 12-19 avril 2010. URL: https://www.un.org/fr/conf/crimecongress2010/pdf/presskitfactsheets8.pdf

3. Francesco SEATZU. Convention des nations unies sur la cybercriminalite : une avancee au prix des droits humains? 2025. URL: https://revue-jadie.eu/article/view/9181

4. United Nations Convention against Cybercrime. New York, 24 December 2024. URL: https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html#art35

Сергєєва Діана Борисівна, *доктор юридичних наук, професор, головний науковий співробітник Національної академії Служби безпеки України*

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ РЕЙДЕРСЬКИХ ЗАХОПЛЕНЬ, УЧИНЕНИХ ІЗ ВИКОРИСТАННЯМ СУДОВИХ РІШЕНЬ І ДЕРЖАВНОЇ РЕЄСТРАЦІЇ

Рейдерські захоплення належать до складних для виявлення, розслідування та доказування кримінальних правопорушень, оскільки протиправний результат у таких випадках нерідко досягається не шляхом відкритого фізичного заволодіння майном, а через послідовне використання зовні правомірних юридичних процедур. Особливо складними є механізми, у яких для встановлення контролю над підприємством, його корпоративними правами, нерухомістю чи іншими активами використовуються судові рішення, нотаріальні дії та державна реєстрація. У таких випадках протиправне заволодіння маскується під реалізацію цивільних, господарських або корпоративних прав, а внесення відповідних відомостей до державних реєстрів створює формальну юридичну підставу для зміни керівника, складу учасників юридичної особи, власника майна або іншого носія корпоративного чи майнового контролю.

Проблематика рейдерства та засобів протидії йому тривалий час досліджується у вітчизняній юридичній науці. У працях О. Г. Кальмана та М. А. Погорецького обґрунтовано комплексний характер причин рейдерства та необхідність системних заходів протидії [2]. У наших попередніх дослідженнях показано подальшу трансформацію рейдерських механізмів, посилення ролі державної реєстрації, цифрових технологій і професійних учасників юридичних процедур, а також необхідність формування спеціалізованих криміналістичних рекомендацій щодо розслідування таких посягань [10; 11].

На нашу думку, рейдерське захоплення, учинене з використанням судових рішень і державної реєстрації, у криміналістичному аспекті доцільно розуміти як багатоетапний, функціонально пов'язаний механізм протиправного встановлення юридичного та фактичного контролю над підприємством, корпоративними правами або майновими активами, у якому судове провадження,