# ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

**С. БУЯДЖИ**
***здобувач кафедри теорії, історії держави і права та міжнародного права Інституту права імені Володимира Сташиса Класичного приватного університету***

Збільшення кількості кіберзагроз у нашій державі робить все актуальнішим питання оптимізації правового регулювання зазначеної сфери. У світлі євроінтеграційних процесів важливою для України є демонстрація того, що ми готові протистояти загрозам цього виду злочинності, який так стрімко зростає. Окрім того, в сучасних умовах важливою є готовність приймати необхідні зміни, що відповідатимуть європейським і світовим стандартам.

Постійний розвиток правового регулювання боротьби з кіберзлочинністю в Україні є важливим з огляду на такі фактори. По-перше, на сьогодні практично всі державні та недержавні процеси відбуваються із застосуванням інструментів кіберпростору. По-друге, в умовах неоголошеної війни, у якій вимушена брати участь Україна, віртуальний простір є одним із фронтів, у якому наша держава має слабкі показники. По-третє, рівень усвідомлення загрози кіберзлочинів та їх небезпечності у суспільстві все ще є невисоким. За таких умов проблема перспектив правового регулювання боротьби з кіберзлочинністю в Україні є однією з першочергових для науково-го дослідження з метою забезпечення належних змін на практиці.

Важливий внесок у розвиток інституту правового регулювання боротьби з кіберзлочинністю зробили такі учені, як: В. Бутузов, В. Василевич, В. Дзондзюк, Д. Дубов, О. Користін, О. Луньова, О. Манжай, М. Ожеван, Ю. Онищенко, О. Орлов, С. Шепетько та ін. Проте кількість таких праць — незначна. Крім того, переважна більшість із них належним чином не розкриває тему нашого дослідження, що і зумовлює актуальність обраної проблематики.

Мета статті полягає у характеристиці перспектив правового регулювання боротьби з кіберзлочинністю в Україні. Це передбачає виконання таких завдань: з'ясування сутності правового регулювання боротьби з кіберзлочинністю в Україні; характеристику ознак національних нормативно-правових актів, що здійснюють правове регулювання боротьби з кіберзлочинністю; розкриття змісту перспектив правового регулювання боротьби з кіберзлочинністю в Україні.

На нашу думку, національним правовим регулюванням боротьби з кіберзлочинністю в Україні є впорядкування поведінки осіб у кіберпросторі та керу-

© С. Буяджи, 2017

вання нею, що здійснюється за допомогою встановлених, санкціонованих чи ратифікованих державою законних і підзаконних нормативно-правових актів, а також міжнародних договорів та угод, укладених Україною, які поширюються на всі випадки деструктивної діяльності у кіберпросторі, та усіх суб'єктів, що вступили у нормативно-регламентовані суспільні відносини.

Вважаємо, що ознаками національних нормативно-правових актів, які здійснюють правове регулювання боротьби з кіберзлочинністю, мають бути:

1) системність — на сьогодні створено розгалужену систему законних і підзаконних нормативно-правових актів, які в єдності забезпечують кібербезпеку України на цьому етапі. Система функціонує таким чином: забезпечення кібербезпеки України Конституція України визначає однією з найважливіших функцій держави. У Кримінальному кодексі України (далі — КК України) визначено негативні діяння, пов'язані з цим явищем, за які встановлено кримінальну відповідальність та санкції для правопорушників. Численні закони України регламентують суспільні відносини у цій сфері. Підзаконні нормативно-правові акти закріплюють механізми регламентації таких відносин і вектори подальшого розвитку всієї сфери. Тобто правове регулювання боротьби з кіберзлочинністю є можливим лише за умови системного втілення приписів проаналізованих законодавчих актів;

2) всеохопливість — нормативно-правові акти, прийняті у цій сфері, охоплюють регламентацію питань кібербезпеки держави, кіберпростору, захист прав та інтересів громадян, протидії комп'ютерній злочинності та комп'ютерному тероризму тощо. Тобто боротьба з кіберзлочинністю є процесом, який передбачає комплексне застосування заходів, а нормативно-правове регулювання забезпечує закріплення відповідних механізмів;

3) перспективність — деякі підзаконні нормативно-правові акти прийнято з метою встановлення векторів для подальшої еволюції зазначеної сфери. Тому сучасний стан національного правового регулювання боротьби з кіберзлочинністю свідчить про те, що цей інститут все ще перебуває на початкових етапах свого розвитку;

4) деталізація — боротьба з кіберзлочинністю водночас розглядається у декількох аспектах, зокрема як протиправне діяння, передбачене нормами КК України, що спричинило шкоду громадянам України; напрям державної політики; загроза національній безпеці; один зі способів консолідації громадян тощо.

Враховуючи ту обставину, що на сьогодні все ще відсутнє єдине розуміння того, що ж являє собою кіберзлочинність, зазначимо: регламентація цього інституту здійснюється на порівняно невисокому рівні. При цьому нагальною проблемою є неузгодженість між такими нормативно-правовими актами та відсутність єдиного понятійного апарату.

Аналіз праць вітчизняних учених продемонстрував, що чіткий та актуальний перелік перспектив розвитку правового регулювання боротьби з кіберзлочинністю в Україні наразі відсутній. Проте до окремих аспектів вони все ж звертаються, тому вважаємо за можливе проаналізувати найвдаліші з них та сформулювати єдину систему перспектив правового регулювання боротьби з кіберзлочинністю в Україні станом на сьогодні.

Наприклад, О. Йона та М. Казакова зазначають про один зі стратегічних напрямів, а саме «налагодження в Україні системи співробітництва з іншими державами, що обумовлено необхідністю обміну досвідом на міжнародному рівні» [1, 60]. Із такою позицією варто погодитися з огляду на те,

що Україна прагне стати частиною європейських і світових процесів. За таких умов співпраця із більш досвідченими у цьому питанні країнами є вкрай необхідною. Оскільки на світовому рівні боротьба з кіберзлочинністю розпочалася майже на десятиліття раніше, ніж в Україні, перейняття досвіду розвинутіших країн очевидно ще довгий час буде на першій сходинці у переліку основних перспектив правового регулювання боротьби з кіберзлочинністю у нашій державі.

В. Марков зазначає, що «до основних проблем виявлення, розкриття та розслідування "транскордонних" злочинів із використанням глобальної мережі Інтернет варто віднести територіальну розподільність слідів злочину та зберігання їх протягом невеликого проміжку часу» [2, 108]. Інакше кажучи, при визначенні місця вчинення кіберзлочинів імовірні проблеми, оскільки злочинці у всесвітній мережі Інтернет можуть діяти анонімно, а будь-які докази чи сліди протиправної діяльності безслідно видаляються. Тому для розслідування таких злочинів необхідною є взаємодія оперативних підрозділів на усіх рівнях, зокрема й на міждержавному із представниками правоохоронних органів інших країн. Тобто, з огляду на зазначені проблеми, можна спостерігати перспективу ліквідації кордонів між державами у питаннях боротьби з кіберзлочинністю.

Вперше це проявилося на початку XXI ст., коли було прийнято низку міжнародних нормативно-правових актів, які і сьогодні становлять основу європейського та світового законодавства про кіберзлочинність: Конвенцію Організації Об'єднаних Націй (далі — ООН) проти транснаціональної організованої злочинності від 15 листопада 2000 р.; Віденську декларацію про злочинність і правосуддя: відповіді на виклики XXI століття (ООН) від 17 квітня 2000 р.; Конвенцію про взаємодопомогу в кримінальних справах між державами — членами Європейського Союзу; Конвенцію про кіберзлочинність від 23 листопада 2001 р., ратифіковану Україною 7 вересня 2005 р.; Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи; Угоду про співробітництво держав — учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації; різноманітні рекомендації Ради Європи. Це стало першим кроком в об'єднанні зусиль міжнародної спільноти у питанні боротьби з кіберзлочинністю. Наступний крок полягав у прийнятті міждержавних угод щодо співробітництва і багатостороннього сприяння боротьби з кіберзлочинністю. Тобто встановлення співпраці на міжнародному рівні розвивалося поступово і на сьогодні вже потребує переходу на якісно новий рівень. Серйозні зміни у законодавчому регулюванні переважно пов'язуються із виникненням нових форм кіберзлочинності.

Тож можна резюмувати, що побудову системи перспектив правового регулювання боротьби з кіберзлочинністю в Україні варто здійснювати з обов'язковим урахуванням таких положень: 1) у нашій державі розпочато процес інтеграції міжнародних нормативно-правових актів у сфері боротьби з кіберзлочинністю у вітчизняне законодавство; 2) Україна співпрацює, проте все ще не досить активно, із зарубіжними державами у питаннях, пов'язаних із розслідуванням кіберзлочинів. Тому подальший розвиток цього інституту варто пов'язати з удосконаленням законодавчої бази та підвищенням взаємодії відповідних підрозділів органів внутрішніх справ на міжнародному рівні — із правоохоронними органами інших держав, що полягатиме у наданні всебічної допомоги в питаннях подолання кіберзлочинності.

Також звернемо увагу на один із негативних аспектів розвитку правового регулювання боротьби з кіберзлочинністю в Україні, на який вказав О. Вінер, а саме: збільшення рівня контролю за користувачами мережі Інтернет [3]. Як приклад можна навести нещодавню ситуацію. 27 червня 2017 р. Україна зазнала масових кібератак шляхом впливу на комп'ютерні системи невідомого на той момент вірусу. У результаті вірус *«Petya.A»*, або *«mbr locker 256»,* спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Негативний вплив було здійснено навіть на веб-ресурси Кіберполіції та Служби спецзв'язку України, що є вагомою проблемою, адже ці органи є суб'єктами боротьби з кіберзлочинністю у нашій державі [4]. Атака продемонструвала недоліки та вразливість національного правового регулювання зазначеної проблеми, а також відсутність у вітчизняній науці та практиці відповіді на запитання: якими є елементи зазначеного механізму? Зокрема, внаслідок цього цілком вірогідним є посилення заходів щодо підвищення ефективності спецслужб шляхом нормативного та фактичного зменшення обсягу прав і свобод, якими наділяються громадяни України.

На основі наведеного вище основною перспективою ми вбачаємо ліквідацію кордонів між державами у питаннях боротьби з кіберзлочинністю.

Кіберзлочинність — це міжнародна проблема, оскільки кіберпростір, як об'єкт її посягання, не обмежується державними кордонами. Саме тому для протидії цим негативним явищам має бути залучена максимальна кількість країн, безвідносно географічного положення, рівня соціально-економічного та технічного розвитку, а також рівня прийнятого національного законодавства, оскільки кіберзлочинець може географічно перебувати та вчиняти злочини навіть у найбільш віддаленому куточку світу. Саме тому технологічно розвиненіші держави повинні мати можливість допомагати менш розвиненим у питаннях запобігання і розслідування кіберзлочинів.

Міжнародне право передбачає низку підстав для визначення юрисдикції за територіальним принципом чи принципом громадянства. Більшість із них закріплені у міжнародних нормативно-правових актах, присвячених запобіганню кіберзлочинності. Водночас є й норми, які надають суб'єктам міжнародного права певну свободу у таких правовідносинах. Наприклад, у Конвенції про кіберзлочинність міститься норма, яка надає право учасникам на здійснення доступу до публічно доступних комп'ютерних даних, які зберігаються, не отримуючи дозволу від іншої сторони, незалежно від того, де вони розміщені територіально; здійснювати доступ або отримувати за допомогою комп'ютерної системи, яка перебуває на її території, комп'ютерні дані, які зберігаються і містяться в іншої сторони, якщо сторона отримує законну і добровільну згоду особи, яка має законні повноваження розкривати їх такій стороні за допомогою такої комп'ютерної системи [5].

Наявність лише зазначеної норми свідчить про нерозвиненість правової бази попередження і регулювання негативного явища кіберзлочинності, незважаючи на те, що, на думку усіх країн Європи, їхнє національне законодавство забезпечує достатню основу для криміналізації та переслідування екстериторіальних кіберзлочинів. О. Орлов та Ю. Онищенко у цьому контексті зазначають, що «в законодавстві численних країн закріплено ідею про те, що для визнання територіальної юрисдикції всередині країни повинно бути здійснено не обов'язково "весь" злочин. Тобто територіальна прив'язка може бути здійснена щодо елементів, наслідків діяння чи місцеперебування комп'ютерних систем або даних, які

використовувалися для скоєння злочину. При виникненні конфліктів між державами, вони вирішуються шляхом проведення взаємних консультацій» [6, 19]. Інакше кажучи, на сьогодні країни не вбачають необхідності у встановленні додаткових заходів у кіберпросторі. За сучасних умов достатніми є форми юрисдикції за територіальною ознакою та згідно з громадянством, що практично завжди може забезпечити зв'язок між кіберзлочинами та хоча б однією державою. Проте розвиток кіберзлочинів та поява нових інструментів протиправного впливу на суспільний порядок можуть докорінно все змінити. Як ми вже зазначали, специфіка кіберзлочинів полягає у тому, що знищення будь-яких доказів чи слідів протиправної діяльності є можливим у найкоротші строки. За умови, коли ця можливість ще зменшиться, світова спільнота потребуватиме швидких дій, а ліквідація кордонів між державами у питаннях боротьби з кіберзлочинністю має забезпечити цю швидкість.

Ця перспектива є можливою за умови втілення таких завдань:

1) стандарти законодавства про боротьбу з кіберзлочинністю мають бути єдиними для усіх країн світу. На сьогодні у міжнародному праві наявний значний масив нормативно-правових актів, які регламентують боротьбу з кіберзлочинністю. Проте їхня дія поширюється лише на окремі групи країн та існує низка бюрократичних перепон, що не дають змогу оперативно розслідувати випадки кіберзлочинів, здійснених із території інших держав чи за участю іноземних громадян. Тому головним завданням є залучення до цього процесу якомога більшої кількості країн і пришвидшення процесу ратифікації ними усіх необхідних нормативно-правових актів;

2) забезпечення обміну інформацією щодо кібертерористичних організацій та кібертерористів, зокрема їх особистими та біографічними даними. Такий напрям можна реалізувати шляхом створення єдиної бази даних для спецслужб світу та забезпечити автоматизований обмін даними між правоохоронними органами країн щодо осіб, які мають судимість за вчинення кіберзлочинів чи підозрюються у здійсненні шкідливої протиправної діяльності у кіберпросторі;

3) чітка регламентація координування відповідних підрозділів правоохоронних органів державами світу, що буде здійснюватися за допомогою прийнятого законодавства. Інакше кажучи, основним завданням є забезпечення оперативності реагування правоохоронців різних держав на кіберзагрози. Такий напрям, на нашу думку, можливо реалізувати шляхом внесення змін до Конвенції про кіберзлочинність [5]. Так, на сьогодні вона передбачає можливість міжнародного співробітництва у сфері боротьби з кіберзлочинністю без укладення міжнародних угод. Наприклад, нині кожна сторона надає одна одній взаємну допомогу у найширшому обсязі з метою розслідування або переслідування кіберзлочинів, а держави, які не є сторонами цієї Конвенції, вимушені для початку надсилати запити про таку допомогу, які можуть бути відхилені за бажанням іншої держави. Тому першим і головним завданням є забезпечення ратифікації Конвенції про кіберзлочинність максимальною кількістю держав. По-друге, необхідним є прийняття єдиного законодавства, що регламентуватиме діяльність підрозділів правоохоронних органів більшості держав світу. Таким нормативно-правовим актом може бути Конвенція проти транснаціональної кіберзлочинності, мета якої полягатиме у сприянні співробітництву в справі більш ефективного попередження та боротьби з транснаціональною організованою злочинністю.

Таким чином, підбиваючи підсумки, варто зазначити, що на сучасному етапі

проблема кіберзлочинності набула глобального виміру та становить серйозну загрозу усім без винятку суспільним відносинам у державі. Майбутній розвиток досліджуваного інституту вбачаємо у вирішенні існуючих на сьогодні проблем, зокрема: нормативного та понятійного характеру; недостатнього наукового аналізу цього питання; реалізації позитивного досвіду зарубіжних держав тощо. Оскільки кіберпростір не має меж, більшість існуючих проблем повинні вирішуватися на міждержавному рівні. Тож дослідження перспектив правового регулювання боротьби з кіберзлочинністю в Україні продемонструвало, що еволюція цієї тематики має бути багатовекторною, оскільки проблем у його регламентації залишається чимало.

**ВИКОРИСТАНІ МАТЕРІАЛИ**


1. *Йона О. О.* Світові тенденції боротьби з кіберзлочинністю / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2013. — № 15 (1). — С. 59–61.
2. *Марков В. В.* До питання щодо зарубіжного досвіду протидії кіберзлочинності / В. В. Марков // Право і Безпека. — 2015. — № 2. — С. 107–113.
3. *Вінер О.* В тенетах світової павутини: тенденції розвитку кібербезпеки у 2016 році / О. Вінер [Електронний ресурс]. — Режим доступу : https://defence-ua.com/index.php/statti/562-v-tenetakh-/svitovoyi-pavutyny-tendentsiyi-rozvytku-kiberbezpeky-u-2016-r
4. *Хакерська* атака в Україні: як працює вірус Petya.A і що робити? [Електронний ресурс]. — Режим доступу : http://24tv.ua/hakerska_ataka_v_ukrayini_virus_petya_a_yak_pratsyuye_i_shho_robiti_/n835033
5. *Конвенція* про кіберзлочинність від 23 листопада 2001 р. // Офіційний вісник України. — 2007. — № 65. — Ст. 2535.
6. *Орлов О. В.* Міжнародна співпраця у сфері боротьби з кіберзлочинністю / О. В. Орлов, Ю. М. Онищенко // Теорія та практика державного управління. — 2013. — Вип. 4. — С. 17–23.


**REFERENCES**


1. Yona O. O., Kazakova N. F. Svitovi tendentsiyi borotby z kiberzlochynnistyu [World trends in the fight against cybercrime], *Visnyk Skhidnoukrayinskoho natsionalnoho universytetu imeni Volodymyra Dalya,* 2013, no. 15 (1), pp. 59–61.
2. Markov V. V. Do pytannya shchodo zarubizhnoho dosvidu protydiyi kiberzlochynnosti [To the issue of foreign experience in combating cybercrime], *Pravo i Bezpeka,* 2015, no. 2, pp. 107–113.
3. Viner O. V tenetakh svitovoyi pavutyny: tendentsiyi rozvytku kiberbezpeky u 2016 rotsi [In the World Wide Web: trends in cybersecurity in 2016]. Available at: https://defence-ua.com/index.php/statti/ /562-v-tenetakh-svitovoyi-pavutyny-tendentsiyi-rozvytku-kiberbezpeky-u-2016-r
4. Khakerska ataka v Ukrayini: yak pratsyuye virus Petya.A i shcho robyty? [Hacker attack in Ukraine: how Petya.A virus works and what to do?]. Available at: http://24tv.ua/hakerska_ataka_v_ukrayini_virus_/petya_a_yak_pratsyuye_i_shho_robiti_n835033
5. Konventsiya pro kiberzlochynnist vid 23 lystopada 2001 r. [Convention on Cybercrime], Ofitsiynyy /visnyk Ukrayiny, 2007, no. 65, Article 2535.
6. Orlov O. V., Onyshchenko Yu. M. Mizhnarodna spivpratsya u sferi borotby z kiberzlochynnistyu [International cooperation in the field of combating cybercrime], *Teoriya ta praktyka derzhavnoho upravlinnya,* 2013, no. 4, pp. 17–23.


*Рекомендовано до друку кафедрою теорії, історії держави і права та міжнародного права Інституту права імені Володимира Сташиса Класичного приватного університету.*

---

**Буяджи С. Перспективи правового регулювання боротьби з кіберзлочинністю в Україні**

***Анотація.*** У статті здійснюється аналіз перспектив правового регулювання боротьби з кіберзлочинністю в Україні. Надається тлумачення поняття «національне правове регулювання боротьби з кіберзлочинністю в Україні». Наводиться перелік ознак національних нормативно-правових актів, що здійснюють правове регулювання боротьби з кіберзлочинністю. Досліджуються позиції вчених щодо напрямів розвитку правового регулювання боротьби з кіберзлочинністю. Визначаються перспективи правового регулювання боротьби з кіберзлочинністю і характеризується зміст кожної з них. Розкриваються проблеми їх втілення.

***Ключові слова:*** правове регулювання, кіберзлочинність, кібератака, перспектива, боротьба з кіберзлочинністю, нормативно-правові акти.

**Буяджы С. Перспективы правового регулирования борьбы с киберпреступностью в Украине**

***Аннотация.*** В статье проводится анализ перспектив правового регулирования борьбы с киберпреступностью в Украине. Предоставляется толкование понятия «национальное правовое регулирование борьбы с киберпреступностью в Украине». Приводится перечень признаков национальных нормативно-правовых актов, которые осуществляют правовое регулирование борьбы с киберпреступностью. Исследуются позиции ученых по направлениям развития правового регулирования борьбы с киберпреступностью. Определяются перспективы правового регулирования борьбы с киберпреступностью и характеризуется содержание каждой из них. Раскрываются проблемы их воплощения.

***Ключевые слова:*** правовое регулирование, киберпреступность, кибератака, перспектива, борьба с киберпреступностью, нормативно-правовые акты.

**Buiadzhy H. Prospects for Legal Regulation of the Fight Against Cybercrime in Ukraine**

***Annotation.*** The article analyzes the prospects of legal regulation of the fight against cybercrime in Ukraine. Author's interpretation of the concept «national legal regulation of the fight against cybercrime in Ukraine» is given. Explores the list of features of the national normative-legal acts implementing the legal regulation of the fight against cybercrime. Examined positions of scientists concerning directions of development of legal regulation of the fight against cybercrime. Characterizes the prospects of legal regulation of combating cybercrime and determines the content of each of them. Reveales problems of their implementation.

***Key words:*** legal regulation, cybercrime, cyber attack, prospect, fight against cybercrime, legal acts.