Бейкун А.Л.,
кандидат юридичних наук, доцент, доцент кафедри правового забезпечення та правоохоронної діяльності,
Київський інститут Національної гвардії України
(м. Київ, Україна)

Дерягін О.С.,
здобувач вищої освіти факультету забезпечення державної безпеки,
Київський інститут Національної гвардії України
(м. Київ, Україна)

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ ТА ПРАВОВА ПРОБЛЕМАТИКА ФОРМУВАННЯ ІНСТИТУЦІЙНОЇ СТРУКТУРИ КІБЕРБЕЗПЕКИ ЯК ЕЛЕМЕНТУ СУЧАСНОЇ СИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

24 лютого 2022 року Україна зіткнулася з новоформатним викликом для свого існування – повномасштабна неспровокована збройна агресія з боку російської федерації здійснювалася всіма можливими «гібридними» засобами, включаючи кібератаки. І на сьогодні постійна кіберзагроза залишається важливим фактором впливу на національну систему кібербезпеки, а також є визначальним елементом для діяльності українських кібербезпекових стейкхолдерів [1, с. 4].

Крім того, як відомо, сучасний світ характеризується стрімким розвитком інформаційно-комунікаційних технологій, що надають безпрецедентні можливості для обміну даними та розширюють глобальний комунікаційний простір. Віртуальний простір став невід'ємною частиною нашого повсякденного життя, впливаючи на всі сфери суспільних відносин. Цифрова трансформація змінила не лише суспільні відносини, але й характер загроз безпеці держави, суспільства та окремих громадян, що, відповідно, зумовлює необхідність розробки ефективних механізмів забезпечення кібербезпеки. Комп'ютеризація суспільних відносин призвела до появи нових форм правопорушень, що реалізуються у кіберпросторі та становлять загрозу для національної безпеки України, призводячи до необхідності реформування правового регулювання цих відносин [2, с. 15].

Питання кібербезпеки як складової національної безпеки держави набуває все більшого значення в умовах сучасних глобалізаційних процесів. За даними Національного координаційного центру кібербезпеки, кількість кібератак на українські інформаційні системи зросла на 35% протягом останнього року повномасштабної війни. Відповідно, правове регулювання

відносин у сфері кібербезпеки вимагає глибокого наукового осмислення та систематизації, особливо з огляду на міждисциплінарний характер цього явища, що охоплює технічні, соціальні та правові аспекти [1, с. 12].

Розгляд кібербезпеки як елемента правової безпеки передбачає аналіз взаємозв'язку між технологічними аспектами захисту інформації та правовими механізмами протидії кіберзагрозам у контексті забезпечення національної безпеки країни. Нормативно-правове забезпечення кібербезпеки в Україні має відповідати міжнародним стандартам і враховувати особливості національної правової системи, формуючи цілісну концепцію правового регулювання відносин у кіберпросторі. Пріоритетним завданням держави у цій сфері є, як вбачається, створення ефективної системи захисту інформаційних ресурсів та критичної інфраструктури від кібератак, що потребує не лише технологічних рішень, але й відповідного законодавчого забезпечення.

Національна система кібербезпеки України перебуває на етапі активного формування, що супроводжується розробкою та вдосконаленням законодавчої бази, формуванням інституційної структури та впровадженням міжнародних стандартів. У зв’язку з цим варто відмітити наукові надбання таких дослідників: Г.К. Авдєєвої, О.А. Баранова, В.М. Бутузова, І.І. Васильковського, В.І. Гур’єва, Д.Б. Мехеди, Ю.М. Ткача, І.В. Федака, І.В. Фірсової та інших.

У той же час, як законодавець, так і галузева теорія визначають кібербезпеку як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [3, с. 45].

Проте, реалізація цього визначення на практиці потребує комплексного підходу, що враховує динамічний характер кіберзагроз та їх транскордонний характер.

Система забезпечення кібербезпеки є багаторівневою і включає нормативно-правове регулювання, організаційні заходи, технічні засоби захисту інформації та підготовку фахівців у галузі кібербезпеки. Правове регулювання кібербезпеки в Україні ґрунтується на Конституції України, міжнародних договорах, законах України: «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» та інших нормативно-правових актах. Особливе значення має програмний документ - Стратегія кібербезпеки України, прийнята у 2021 році та затверджена Указом Президента України 26 серпня 2021 року № 447/2021, яка визначає пріоритети та напрями забезпечення кібербезпеки з урахуванням реальних та потенційних кіберзагроз.

Аналіз науковцями-правниками як теоретичних напрацювань, так і нормативно-правової бази у сфері кібербезпеки дозволяє виділити декілька ключових проблем, що потребують вирішення. По-перше, відсутність єдиного

підходу до визначення поняття «кібербезпека» та суміжних термінів у законодавстві України. Різні нормативно-правові акти містять різні визначення, що створює термінологічну неузгодженість та ускладнює правозастосування. По-друге, недостатня координація діяльності державних органів, відповідальних за забезпечення кібербезпеки, що призводить до дублювання функцій та неефективного використання ресурсів. По-третє, відсутність чітких механізмів взаємодії між державним та приватним секторами у сфері кібербезпеки, що ускладнює обмін інформацією про кіберзагрози та реагування на інциденти. По-четверте, недостатнє врахування міжнародних стандартів та найкращих практик у сфері кібербезпеки при розробці національного законодавства [4, с. 278; 5, с. 270-271; 6, с. 73].

Для подолання зазначених проблем науковцями аксіомно висувається теза:

- необхідності вдосконалення законодавчої бази у сфері кібербезпеки,
- забезпечення координації діяльності державних органів,
- сприяння розвитку державно-приватного партнерства у сфері захисту,
- впровадження міжнародних стандартів захисту баз даних,
- підвищення рівня кіберграмотності населення та підготовка фахівців у галузі кібербезпеки.

Так, дослідник О. Баранов зазначає, що: «формування ефективної системи кібербезпеки потребує не лише технологічних рішень, але й відповідного правового регулювання, яке має забезпечити баланс між захистом інформаційних ресурсів та дотриманням прав і свобод громадян» [7, с. 78].

Крім того, аналіз зарубіжного досвіду правового регулювання кібербезпеки, запропонований нам К.Є. Ковальовим, дозволяє виділити декілька моделей організації системи кібербезпеки, які можуть бути адаптовані до українських реалій. Централізована модель, характерна для країн Європейського Союзу, передбачає створення єдиного державного органу, відповідального за координацію діяльності у сфері кібербезпеки. Децентралізована модель, характерна для США, базується на розподілі повноважень між різними державними органами та активному залученні приватного сектора. Змішана модель, що поєднує елементи централізованої та децентралізованої моделей, є найбільш перспективною для України, оскільки дозволяє забезпечити баланс між централізованим управлінням та гнучкістю реагування на кіберзагрози [8, с. 162-165].

Безумовно, що одним із ключових аспектів правового регулювання кібербезпеки є встановлення відповідальності за кіберзлочини. Кримінальний кодекс України містить низку статей, що передбачають відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Проте, динамічний характер кіберзлочинності вимагає постійного оновлення законодавства та адаптації його до нових форм кіберзагроз. Крім того, транскордонний характер кіберзлочинності зумовлює необхідність

міжнародного співробітництва у розслідуванні та переслідуванні кіберзлочинців [4, с. 280; 5, с. 273-274; 9, с. 36].

Важливим елементом системи правової безпеки у кіберпросторі є захист персональних даних. В умовах цифрової трансформації суспільства обсяг персональних даних, що обробляються в інформаційних системах, постійно зростає, що створює додаткові ризики для їх безпеки. Законодавство України у сфері захисту персональних даних має відповідати міжнародним стандартам, зокрема, Загальному регламенту про захист даних (GDPR) Європейського Союзу. Це дозволить забезпечити високий рівень захисту персональних даних громадян України та сприятиме інтеграції України до єдиного цифрового ринку ЄС.

Окремої уваги заслуговує питання захисту критичної інформаційної інфраструктури, яка є основою для функціонування стратегічно важливих галузей економіки та державного управління. Закон України «Про основні засади забезпечення кібербезпеки України» визначає об'єкти критичної інформаційної інфраструктури та встановлює вимоги до їх захисту. Проте, практична реалізація цих вимог потребує розробки детальних підзаконних актів, які б визначали конкретні заходи захисту та відповідальність за їх порушення.

Проблема кібертероризму та використання кіберпростору для ведення інформаційної війни набуває особливого значення в умовах повномасштабної збройної агресії проти України, але з використанням ново форматних «гібридних» елементів, що, на думку, агресора, повинно посилити уразливість відповідних об’єктів деструктивного впливу. Відповідно, як вбачається, необхідно розробити правові механізми протидії таким загрозам, що включатимуть: як технічні засоби захисту інформаційних ресурсів, так і правові засоби притягнення до відповідальності осіб, причетних до кібератак. Так, В. Бутузов зазначає, що «кібертероризм становить серйозну загрозу для національної безпеки України, оскільки може призвести до дестабілізації роботи стратегічно важливих об'єктів інфраструктури та порушення функціонування державних інституцій» [10, с. 156].

Міжнародно-правове співробітництво у сфері кібербезпеки є необхідною умовою ефективної протидії кіберзагрозам, враховуючи їх транскордонний характер. Україна є учасницею Конвенції про кіберзлочинність, яка встановлює єдині підходи до кваліфікації кіберзлочинів та процедур розслідування. Проте, необхідно розширювати співробітництво з міжнародними організаціями та іншими державами у сфері кібербезпеки, зокрема, шляхом участі в міжнародних навчаннях, обміну інформацією про кіберзагрози та координації діяльності правоохоронних органів.

Важливим аспектом забезпечення кібербезпеки є розвиток державно-приватного партнерства. Приватний сектор (зокрема, оператори критичної інфраструктури, провайдери інтернет-послуг, розробники програмного забезпечення тощо) відіграє ключову роль у забезпеченні кібербезпеки. Як вбачається, необхідно розробити правові механізми, які б стимулювали приватний сектор інвестувати у кібербезпеку та співпрацювати з державними

органами у протидії кіберзагрозам. Одним із таких механізмів може бути впровадження обов'язкових вимог до кібербезпеки для операторів критичної інфраструктури та створення платформи для обміну інформацією про кіберзагрози.

Підготовка фахівців у галузі кібербезпеки є необхідною умовою для забезпечення належного рівня захисту інформаційних ресурсів. Отже, необхідно розробити освітні програми та стандарти підготовки фахівців з кібербезпеки, які б відповідали сучасним вимогам та міжнародним стандартам. Крім того, важливим є підвищення рівня кіберграмотності населення та формування культури безпечного використання інформаційних технологій.

Отже, сучасний стан кібербезпеки в Україні характеризується наявністю низки проблем, що потребують комплексного вирішення. І аналіз статистичних даних свідчить про зростання кількості та складності кібератак на українські інформаційні системи. За даними Національного координаційного центру кібербезпеки, протягом жовтня 2023- вересня 2024 було зафіксовано понад 1500 кібератак на об'єкти критичної інформаційної інфраструктури України. Найбільш поширеними типами кібератак були DDoS-атаки, фішингові атаки, використання шкідливого програмного забезпечення та соціальна інженерія [1, с. 17].

Нажаль, на даний час правова система України не повністю адаптована до сучасних викликів у сфері кібербезпеки. Наявність прогалин у законодавстві, відсутність чітких механізмів координації діяльності державних органів та недостатнє врахування міжнародних стандартів ускладнюють ефективну протидію кіберзагрозам. Особливо актуальною є проблема правового регулювання відповідальності за кіберзлочини, враховуючи їх транскордонний характер та складність доказування. Відповідно, створення ефективної системи кібербезпеки є стратегічним завданням для України, враховуючи зростаючу роль інформаційно-комунікаційних технологій у всіх сферах суспільного життя та посилення кіберзагроз. Правова складова кібербезпеки має забезпечити баланс між захистом інформаційних ресурсів та дотриманням прав і свобод громадян, створюючи умови для безпечного використання кіберпростору та розвитку інформаційного суспільства.

Список використаних джерел:

1. Річний аналітичний звіт. Жовтень 2023 - вересень 2024. Національний координаційний центр кібербезпеки. 25 лютого 2025. [Інформаційний портал: NATIONAL CYBER SCC]. Київ: НКЦК, 2024. 32 с. URL: https://www.rnbo.gov.ua/files/2024/ NATIONAL_CYBER_SCC/20250109/ Year%20in%20review_UKR_ upd.pdf?fbclid=IwY2xjawI-fZRleHRuA2FlbQIxMA ABHcaZdkgcVIlSJ0eGnBO78 x5xRCDcoBwc J1GKrT4SAVS5reEAtY5u8ssd4w _aem_0xN1oMO3-toIy6vpuA27 mA (дата звернення: 07.05.2025).

2. Інформаційна безпека держави: *навчальний посібник* для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.: іл. URL: https://ir.stu.cn.ua/bitstream/handle/123456789/19246/Inform.%20bezpeka%20derzh.%20New%20booklet%201.pdf?sequence=1&isAllowed=y (дата звернення: 07.05.2025).

3. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. 2022. № 9. С. 44-49. URL: https://opac.library.pl.ua/cgi-bin/koha/opac-detail.pl?biblionumber= 2726814 (дата звернення: 07.05.2025).

4. Васильковський І.І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. № 1–2 (10–11). С. 276-282.

5. Авдєєва Г.К. Використання спеціальних знань у боротьбі з комп'ютерною злочинністю. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка: *матеріали*. 2016. № 1. С. 268-277.

6. Федорченко О.С. Удосконалення координації діяльності суб'єктів забезпечення національної системи кібербезпеки. *Нове українське право*. Вип. 5. 2024. С. 71-77.

7. Баранов О.А. Інтернет речей і кібербезпека: правові аспекти. *Інформація і право*. 2023. № 1(40). С. 76-94.

8. Ковальов К.Є. Інформаційна безпека: міжнародно-правовий аспект. *Інформація і право*. 2023. № 4(47). С. 159-167. URL: https://291624-Текст статті-686548-1-10-20240126.pdf (дата звернення: 07.05.2025).

9. Федак І.В. Криміналістична характеристика злочинів пов'язаних з комп'ютерною технікою та інформаційними системами. *Кваліфікаційна робота (проєкт) на здобуття ступеня вищої освіти «магістр»*. ХДУ. Херсон, 2021. 51 с. URL: https://ekhsuir.kspu.edu/server/api/core/bitstreams/14b73298-5a5d-46df-9503-f38ca86a7ba8/content (дата звернення: 07.05.2025).

10. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): *монографія*. Київ: КИТ, 2021. 320 с.