УДК 349:004.49
DOI 10.33244/2617-4154.3(20).2025.126-134

Н. Б. Новицька,
доктор юридичних наук, професор,
професор кафедри цивільного права та процесу,
Державний податковий університет
email: Natalka_bn_@ukr.net
ORCID 0000-0003-4753-7625;
В. М. Петрик,
кандидат наук з державного управління, доцент,
доцент кафедри кібербезпеки,
ДУ «Київський авіаційний інститут»
email: iszzi_open@ukr.net
ORCID 0000-0003-2662-0876;
М. М. Присяжнюк,
кандидат технічних наук, с.н.с.,
професор спеціальної кафедри № 13,
Воєнна академія імені Євгенія Березняка
email: pnn2006@ukr.net
ORCID 0000-0002-2470-9431

СУЧАСНИЙ СТАН НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

На сьогодні склався новий всесвітній простір інформаційно-цифрової реальності, що співіснує із звичайною фізичною реальністю, але кардинально змінює звичні політичні, економічні й суспільні відносини. Інформація все більше перетворюється на символ політичного впливу й економічного процвітання, стає феноменом геополітичного рангу.

Так, геополітичний авторитет держав на міжнародній арені, його можливості впливати на світові події тепер залежать не тільки від економічної та військової могутності. Усе більшого значення набувають не силові, а інформаційні чинники. За цих умов зростають кіберзагрози національній інформаційній інфраструктурі, відбуваються кібератаки на фінансово-банківську сферу, поширюються акти кібертероризму в глобальній інформаційній мережі з метою підриву традиційних підвалин націй і народів.

Одним з основних джерел загроз національній і міжнародній кібербезпеці залишається російська агресивна політика, яка активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються в гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму й кібердиверсій стосовно національної інформаційної інфраструктури.

У цьому контексті особливого значення набуває формування стійкої системи кіберграмотності населення, зокрема молоді, яка є найбільш активним користувачем цифрових технологій. Освітні програми мають містити компоненти цифрової безпеки, критичного мислення, розпізнавання дезінформації та основ правового регулювання кіберпростору. Такий підхід сприятиме не лише підвищенню рівня національної кіберстійкості, а й формуванню свідомого громадянства, здатного протистояти інформаційним загрозам у новій реальності.

Вжиття заходів щодо ефективної протидії кіберзагрозам, кібертероризму та іншим кіберзлочинам потребує ґрунтовного дослідження відповідного нормативно-правового забезпечення та його вдосконалення.

Ключові слова: *кіберпростір, кіберзагрози, кібертероризм, кіберзлочини, кібердиверсії, кібербезпека, кіберзахист, інформаційна безпека, нормативно-правове забезпечення.*

Постановка проблеми. Стратегією кібербезпеки України, затвердженою Указом Президента України від 26 серпня 2021 року (далі – Стратегія), визначено одним із пріоритетів національної безпеки України – забезпечення кібербезпеки з посиленням спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Стратегія зазначає, що кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів сучасних воєнних дій.

Практична та професійна спрямованість статті зумовлена набуттям знань і вмінь щодо організаційно-правового забезпечення кібербезпеки. Насамперед це знання та вміння, які дають змогу виявляти загрози національній безпеці в кіберсфері, аналізувати сучасний стан системи забезпечення кібербезпеки України й розробляти пропозиції щодо вдосконалення Національної системи кібербезпеки відповідно до сучасних вимог.

Аналіз останніх досліджень. Сучасний стан нормативно-правового забезпечення кібербезпеки розглядався вітчизняними науковцями [1–4], але фрагментарно. На сьогодні системних досліджень з цієї проблематики не існує.

Постановка завдання. Метою статті є розкриття нормативно-правового забезпечення кібербезпеки для його вдосконалення.

Виклад основного матеріалу. В умовах російської воєнної агресії та загроз національній безпеці й територіальній цілісності України важливою для збереження й розбудови незалежної та самостійної української держави є реформа системи національної безпеки й оборони. А це потребує також суттєвого оновлення законодавчої бази.

Початок XXI століття характеризується розвитком і впровадженням новітніх інформаційних і комп’ютерних технологій, що дало змогу прискорити життєво важливі процеси суспільства та послужило створенню принципово нового середовища соціальної активності – кіберпростору, який став міжнародною сферою інфраструктури, інформаційних технологій і взаємозалежних комп’ютерних мереж. За цих умов набувають важливості у світі та в окремих державах питання кібербезпеки та її нормативно-правового забезпечення.

Ключовим різностороннім міжнародним документом з кібербезпеки є Конвенція про кіберзлочинність (Будапештська конвенція), ухвалена Радою Європи 2001 року та ратифікована Законом України від 7 вересня 2005 року № 2824-IV. У цій Конвенції

наведена класифікація комп'ютерних злочинів і рекомендації органам влади держав щодо боротьби з цими злочинами. Ще одним важливим документом у забезпеченні кібербезпеки на міжнародному рівні є Директива про безпеку мереж та інформаційних систем (The Directive on security of network and information systems (NIS Directive), ухвалена Європейським парламентом 2016 року.

Зважаючи на важливість процесів у кіберпросторі та зростання кіберзагроз у цій сфері, світові держави розробляють свої стратегії кібербезпеки та відповідне національне законодавство.

Проте національні стратегії кібербезпеки різних країн розробляються переважно на таких принципах:

– визначення мети та заходів щодо розвитку електронної інформації, її поширення, забезпечення цілісності, конфіденційності й доступності в кіберпросторі;

– забезпечення кібербезпеки як вагомої умови для ефективного функціонування й розвитку суспільства;

– наголошення на здатності інформаційних систем протистояти загрозам у кіберпросторі, що можуть негативно впливати на цілісність, конфіденційність і доступність інформації;

– визначення мети й способів розвитку можливостей держави та розробка відповідної законодавчої бази щодо участі в спільній боротьбі з міжнародною кіберзлочинністю.

Відповідно до Закону України від 2018 року «Про національну безпеки України» кібербезпека є важливою і невід'ємною сферою національної безпеки, а забезпечення кібербезпеки – одним із пріоритетів у системі національної безпеки України.

Правова база кібербезпеки України складається з міжнародних зобов'язань та національного законодавства.

В Україні за час її незалежності закладено законодавчі основи системи забезпечення інформаційної безпеки, зокрема було ухвалено значний масив нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері. Акти національного законодавства, які регламентують діяльність державних органів, організацій і громадян в інформаційній сфері, встановлюють повноваження державних органів щодо забезпечення інформаційної безпеки України.

Нормативну базу забезпечення національної безпеки України в інформаційній сфері доцільно розглядати з урахуванням існуючої ієрархії нормативних актів.

На найвищому рівні стоять норми Конституції України, які закріплюють концептуальні положення національної безпеки України в усіх сферах її існування, а також Концепція національної безпеки України, Стратегія національної безпеки України, Стратегія воєнної безпеки України, Стратегія інформаційної безпеки України, Стратегія кібербезпеки України та Закон України «Про національну безпеку України». Ці документи враховують основні положення міжнародних договорів і угод, ратифікованих Україною, які стосуються її національної безпеки в усіх сферах, зокрема і в інформаційній сфері та кіберсфері.

На другому рівні перебувають закони України конститутивного напряму, де визначаються важливі положення щодо забезпечення національної безпеки в інформаційній сфері: «Про інформацію», «Про державну таємницю», «Про Національну

програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про радіочастотний ресурс», «Про телекомунікації», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист суспільної моралі».

На третьому рівні – закони України інституційного рівня, де закріплені основні форми діяльності державних органів у процесі забезпечення національної безпеки в інформаційній та інших сферах життєдіяльності особи, суспільства й держави (зокрема, «Про оборону України», «Про основи національного спротиву», «Про Збройні Сили України», «Про Службу безпеки України», «Про розвідку України», «Про Службу зовнішньої розвідки України», «Про Державну службу спеціального зв'язку та захисту інформації», «Про поліцію», «Про прокуратуру», «Про правовий режим надзвичайного стану» тощо).

У структурі нормативно-правової бази забезпечення національної безпеки України в інформаційній сфері особливе місце посідають укази й розпорядження Президента України та постанови й декрети Кабінету Міністрів України. Такі нормативні акти є підзаконними й видаються з метою конкретизації та підвищення якості вирішення завдань забезпечення інформаційної безпеки та кібербезпеки, визначених на законодавчому рівні.

Міністерства й відомства України в межах визначеної законами компетенції та відповідальності згідно з нормами чинного законодавства про національну безпеку України, а також відповідно до рішень Президента та Кабінету Міністрів України розробляють відомчі накази, інструкції, положення, спрямовані на реалізацію програм захисту життєво важливих інтересів людини, суспільства, держави в інформаційній сфері та кіберсфері.

Важливу роль у системі законодавства України з питань національної безпеки в інформаційній сфері та кіберсфері відіграють акти нормативного й директивного характеру місцевих органів влади – рішення з питань забезпечення національної безпеки (про боротьбу з наслідками стихійних лих, техногенних аварій і катастроф, про підтримання громадського порядку тощо), які є обов'язковими для виконання всіма підприємствами, установами й організаціями, а також посадовими особами й громадянами на підпорядкованій території.

Останнім часом нашою державою реалізовано ряд серйозних кроків щодо вдосконалення законодавства у сфері кібербезпеки, що знайшло втілення в ухваленні ряду законів, стратегій та інших актів вторинного законодавства з відповідної проблематики.

В Україні триває розбудова національної системи кібербезпеки й кіберзахисту, формування її організаційно-правової та інформаційно-технічної моделі, здатної забезпечити ефективне реагування на латентні й визначені кіберзагрози.

До Переліку документів, що регулюють питання кібербезпеки України, входять законодавчі та концептуальні акти:

1) Закон України «Про національну безпеку України». Із змінами, внесеними згідно із законами: від 4 березня 2020 року № 522-IX та від 16.07.2021 № 1702-IX – вводиться в дію з 1 січня 2022 року; від 16 листопада 2021 року № 1882-IX;

2) Стратегія національної безпеки України. Уведена в дію Указом Президента України від 14 вересня 2020 року № 392/2020;

3) Закон України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України». Із змінами, внесеними згідно із законами: від 21 червня 2018 року № 2469-VIII та внесеними змінами згідно із законами до 2022 року;

4) Стратегія кібербезпеки України. Уведена в дію Указом Президента від 26 серпня 2021 року № 447/2021;

5) План реалізації Стратегії кібербезпеки України. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України». Введено в дію Указом Президента України від 1 лютого 2022 року № 37/2022;

6) Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури. Затверджено постановою Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;

7) Закон України від 2 жовтня 1992 року № 2657-XII «Про інформацію». Введено в дію постановою Верховної Ради України від 2 жовтня 1992 року № 2658-XII. Із внесеними змінами згідно із законами до 2025 року;

8) Закон України від 5 липня 1994 року № 80/94-ВР «Про захист інформації в інформаційно-комунікаційних системах». Введено в дію Постановою Верховної Ради України від 5 липня 1994 року № 81/94-ВР. Із внесеними змінами згідно із законами до 2022 року;

9) Закон України від 21 січня 1994 року № 3855-XII «Про державну таємницю». Введено в дію Постановою Верховної Ради України від 21 січня 1994 року № 3856-XII. Із внесеними змінами згідно із законами до 2025 року;

10) Закон України «Про електронні документи та електронний документообіг». Із змінами, внесеними згідно із законами: від 30 червня 2021 року № 1591-IX – вводиться в дію з 1 серпня 2022 року та від 14 грудня 2021 року № 1953-IX.

До Переліку документів, що регулюють питання кібербезпеки України, належать також Державні стандарти України:

1) Державний стандарт симетричного шифрування інформації «Калина» (ДСТУ 7624: 2015);

2) Державний стандарт хешування «Купина» (ДСТУ 7564: 2014);

3) Державний стандарт електронного цифрового підпису (ДСТУ 4145: 2002) – електронний цифровий підпис на еліптичних кривих;

та галузеві нормативні акти щодо кібербезпеки України:

1) Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури. Затверджено постановою Кабінету Міністрів України від 19 червня 2019 року № 518. Із змінами, внесеними згідно з постановою Кабінету Міністрів України від 02.09.2022 № 991;

2) Меморандум про взаємодію та співробітництво в сфері кібербезпеки й кіберзахисту, спрямовану на попередження, виявлення, ефективне реагування та протидію актуальним кіберзагрозам, підвищення рівня інформаційної безпеки та ситуаційної обізнаності у сфері кібербезпеки та кіберзахисту. Підписаний 2 серпня 2019 року між Центром кіберзахисту Національного банку України та Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України;

3) «Про організацію заходів із забезпечення інформаційної безпеки в банківській системі України». Постанова правління Національного банку України від 28 вересня 2017 року № 95;

4) «Про затвердження Положення про захист інформації та кіберзахист учасниками платіжного ринку». Постанова правління Національного банку України від 19 травня 2021 року № 43. Із змінами, внесеними згідно з постановою Національного банку України від 13.06.2022 № 119;

5) «Про затвердження нормативно-правових актів з питань інформаційної безпеки». Постанова правління Національного банку України від 26 листопада 2015 року № 829;

6) «Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України». Постанова правління Національного банку України від 26 листопада 2015 року № 829;

7) «Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України». Постанова правління Національного банку України від 5 жовтня 2018 року № 106;

8 «Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України». Постанова правління Національного банку України від 13 лютого 2019 року № 38.

Водночас поряд із позитивною динамікою розвитку законодавства України у сфері забезпечення кібербезпеки постає актуальним і важливим питання приведення національного законодавства у відповідність до міжнародних стандартів, нормативно-правових актів, що регулюють питання кібербезпеки, оскільки стратегічним курсом нашої держави є інтеграція до Європейського Союзу та НАТО.

Висновки. Отже, беззаперечним є те, що в умовах російської воєнної агресії в країні має працювати ефективна система забезпечення кібербезпеки, а функції та повноваження відповідних державних органів мають бути закріплені на законодавчому рівні.

Державна політика у сфері кібербезпеки повинна бути зосередженою на задоволенні й захисті життєво важливих інтересів і потреб громадянина, суспільства та держави в кіберпросторі.

Формування перспективного законодавства з метою вдосконалення захисту інтересів особи, суспільства, держави в Україні в умовах сучасної воєнної загрози має враховувати міжнародні стандарти в цій сфері, зокрема вимоги Конвенції про кіберзлочинність. Саме тому державна політика у сфері кібербезпеки значною мірою має спрямовуватися на досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО.

Актуальним залишається імплементація в національне законодавство ряду міжнародних і насамперед європейських нормативних актів у сфері кібербезпеки й протидії кіберзлочинності. Адже наша держава має потенціал бути однією з провідних країн у світі щодо розвитку інформаційних технологій для розвитку українського суспільства в усіх сферах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шпачук В. Суб'єкти державного управління кібербезпекою країни: зарубіжний досвід. *Державне управління: удосконалення та розвиток.* 2019. № 2. URL : http://www.dy.nayka.com.ua/pdf/2_2019/7.pdf

2. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній : практичний посібник. Київ : Консалтингова компанія «СІДКОН», 2021. 372 с.

3. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України : аналітична доповідь. К. : НІСД, 2017. 30 с.

4. Мельник Д. С., Климчук О. О. Реалізація положень Конвенції про кіберзлочинність у правовому полі України. *Інформаційна безпека людини, суспільства, держави. Науково-практичний журнал.* 2009. № 1 (1). С. 39–43.

5. Про національну безпеку України : Закон України, прийнятий 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради України (ВВР).* 2018. № 31. Ст. 241.

6. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text

7. Про Стратегію кібербезпеки України : Указ Президента України від 14 травня 2021 року № 447/2021. URL : https://www.president.gov.ua/documents/4472021-40013

8. План реалізації Стратегії кібербезпеки України. Введено в дію Указом Президента України від 1 лютого 2022 року № 37/2022. URL : https://www.president.gov.ua/documents/372022-41289

9. Про Стратегію національної безпеки України : Указ Президента України від 14 вересня 2020 року № 392/2020. URL : https://www.president.gov.ua/documents/3922020-35037

10. Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19 червня 2019 року № 518. URL : https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8.15

11. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005. URL : https://zakon.rada.gov.ua/laws/show/994_575

REFERENCES

1. Shpachuk B. Subiekty derzhavnoho upravlinnia kiberbezpekoiu krainy: zarubizhnyi dosvid. *Derzhavne upravlinnia: udoskonalennia ta rozvytok.* 2019. № 2. URL : http://www.du.nauka.som.ua/rdf/2_2019/7.rdf

2. Kohut Yu. I. Kiberbezpeka ta ryzyky tsyfrovoi transformatsii kompanii : praktychnyi posibnyk. Kyiv : Konsaltynhova kompaniia "CIDKON", 2021. 372 s.

3. Dubov D. B., Ozhevan M. A. Kiberbezpeka: svitovi tendentsii ta vyklyky dlia Ukrainy : analitychna dopovid. K. : NICD, 2017. 30 s.

4. Melnyk D. C., Klymchuk O. O. Realizatsiia polozhen Konventsii pro kiberzlochynnist u pravovomu poli Ukrainy. *Informatsiina bezpeka liudyny, suspilstva, derzhavy. Naukovo-praktychnyi zhurnal.* 2009. № 1 (1). C. 39–43.

5. Pro natsionalnu bezpeku Ukrainy : Zakon Ukrainy, pryiniatyi 21 chervnia 2018 roku № 2469-VIII. *Vidomosti Verkhovnoi Rady (VVR)*. 2018. № 31. St. 241.

6. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 5 zhovtnia 2017 roku № 2163-VIII. URL : httrs://zakon.rada.gov.ua/laws/show/2163-19#Tekht

7. Pro Stratehiiu kiberbezpeky Ukrainy : Ukaz Prezydenta Ukrainy vid 14 travnia 2021 roku № 447/2021. URL : httrs://www.rresident.gov.ua/dosuments/4472021-40013

8. Plan realizatsii Stratehii kiberbezpeky Ukrainy. Vvedeno v diiu Ukazom Prezydenta Ukrainy vid 1 liutoho 2022 roku № 37/2022. URL : httrs://www.rresident.gov.ua/dosuments/372022-41289

9. Pro Stratehiiu natsionalnoi bezpeky Ukrainy : Ukaz Prezydenta Ukrainy vid 14 veresnia 2020 roku № 392/2020. URL : httrs://www.rresident.gov.ua/dosuments/3922020-35037

10. Pro zatverdzhennia zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury : postanova Kabinetu Ministriv Ukrainy vid 19 chervnia 2019 roku № 518. URL : httrs://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8.15

11. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist : Zakon Ukrainy vid 07.09.2005. URL : httrs://zakon.rada.gov.ua/laws/show/994_575

N. B. Novytska, V. M. Petryk, M. M. Prysyazhnyuk. CURRENT STATE OF THE REGULATORY AND LEGAL FRAMEWORK FOR CYBERSECURITY

Today, a new global space of information and digital reality has emerged, coexisting with the traditional physical reality but fundamentally transforming conventional political, economic, and social relations. Information is increasingly becoming a symbol of political influence and economic prosperity, evolving into a phenomenon of geopolitical significance.

Thus, the geopolitical authority of states on the international stage and their ability to influence global events now depend not only on economic and military power. Non-forceful, informational factors are gaining greater importance. Under these conditions, cyber threats to national information infrastructure are intensifying, cyberattacks on the financial and banking sectors are occurring, and acts of cyberterrorism are spreading across the global information network with the aim of undermining the traditional foundations of nations and peoples.

One of the main sources of threats to national and international cybersecurity remains Russia's aggressive policy, which actively implements the concept of information confrontation. This concept is based on a combination of destructive actions in cyberspace and information-psychological operations, the mechanisms of which are actively used in the hybrid war against Ukraine. Such destructive activity poses a real threat of cyberterrorism and cyber sabotage targeting national information infrastructure.

In this context, the development of a resilient system of cyber literacy among the population, especially youth – who are the most active users of digital technologies – becomes particularly important. Educational programs must include components of digital security, critical thinking, disinformation detection, and the fundamentals of legal regulation of cyberspace. This approach will contribute not only to strengthening national cyber

resilience but also to shaping a conscious citizenry capable of resisting informational threats in the new reality.

Implementing effective measures to counter cyber threats, cyberterrorism, and other cybercrimes requires thorough research of the relevant regulatory and legal framework and its continuous improvement.

Keywords: *cyberspace, cyber threats, cyberterrorism, cybercrimes, cyber sabotage, cybersecurity, cyber protection, information security, regulatory and legal framework.*

Стаття надійшла до редколегії 15 жовтня 2025 року