УДК 341.231.14
DOI https://doi.org/10.32782/2524-0374/2022-5/161

МІЖНАРОДНІ ТА ЄВРОПЕЙСЬКІ ГАРАНТІЇ ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В КІБЕРПРОСТОРІ

INTERNATIONAL AND EUROPEAN GUARANTEES FOR HUMAN RIGHTS IN CYBERSPACE

Цебенко С.Б., к.ю.н., доцент,
доцент кафедри теорії права та конституціоналізму
Інститут права, психології та інноваційної освіти
Національного університету «Львівська політехніка»

Стаття присвячена аналізу актів у сфері кіберпростору на міжнародному та європейському рівнях. Зокрема щодо питань захисту інформаційних прав людини в мережі Інретнет, захисту особових даних особи та можливі злочини у кіберпросторі.

Зазначено, що інформаційні права людини та їх безпека виникають із принципово новим етапом розвитку людства на сучасному етапі цивілізаційного розвитку. У контексті інформаційних прав також розглядається поняття кібербезпеки, яке є самостійним явищем. Хоча часто поняття кібербезпеки розглядається як складова частина національної безпеки.

Кібербезпека є складним правовим явищем, у рамках якого функціонує механізм кіберзахисту. Кіберзахист здійснюється в межах кіберпростору. Кіберпростір – це складне середовище взаємодії людей, програмного забезпечення та послуг у мережі Інтернет та функціонує за підтримки об'єднаних мереж і пристроїв інформаційних та комунікаційних технологій.

У статті проаналізовано низку міжнародних актів у сфері кібербезпеки. Зокрема проаналізовано деякі резолюції Генеральної Асамблеї Організації Об'єднаних Націй, Конвенцію Ради Європи про кіберзлочинність, Стратегію кібербезпеки Європейського Союзу у цифрове десятиліття.

Зроблено висновки, що регулювання кібербезпеки має глобальне значення і відбувається на міжнародному рівні. В Україні є необхідність розробки та постійного удосконалення нормативно-правового регулювання кібербезпеки враховуючи міжнародні рекомендації та ратифіковані акти. Це має бути з метою, зокрема, щоб адекватно запобігати загрозам, які існують в цій сфері. На міжнародному рівні фактично виробляються стандарти безпеки, які повинні дотримуватися на об'єктах критичної інфраструктури, а їх недотримання має означати можливість притягнення винних осіб до юридичної відповідальності.

Ключові слова: права людини, кіберпростір, кібербезпека, кіберзлочин, право на приватне життя, інформаційна безпека.

The article is devoted to the analysis of acts in the field of cyberspace at the international and European levels. In particular, on the protection of human rights information on the Internet, the protection of personal data and possible crimes in cyberspace.

It is noted that information human rights and their security arise with a fundamentally new stage of human development at the present stage of civilizational development. In the context of information rights, the concept of cybersecurity, which is an independent phenomenon, is also considered. Although the concept of cybersecurity is often seen as part of national security.

Cybersecurity is a complex legal phenomenon within which the cybersecurity mechanism operates. Cybersecurity is provided within cyberspace. Cyberspace is a complex environment for people, software and services to interact on the Internet and is supported by integrated networks and information and communication technology devices.

The article analyzes a number of international acts in the field of cybersecurity. In particular, some resolutions of the United Nations General Assembly, the Council of Europe Convention on Cybercrime, the European Union's Cybersecurity Strategy for the Digital Decade were analyzed.

It is concluded that the regulation of cybersecurity is of global importance and takes place at the international level. In Ukraine, there is a need to develop and continuously improve the legal regulation of cybersecurity, taking into account international recommendations and ratified acts. This should be in order, in particular, to adequately prevent the threats that exist in this area. At the international level, safety standards are in fact being developed, which must be observed at critical infrastructure, and non-compliance with them should mean the possibility of bringing the perpetrators to justice.

Key words: human rights, cyberspace, cybersecurity, cybercrime, right to privacy, information security.

Інформаційні права людини та їх безпека виникають із принципово новим етапом розвитку людства на сучасному етапі цивілізаційного розвитку – формуванням інформаційного суспільства, інформаційного простору (зокрема кіберпростору) та відповідно – інформаційної сфери суспільних відносин.

У контексті інформаційних прав науковцями також розглядається поняття кібербезпеки. Інформаційна безпека – це безпека інформації про фізичну особу, юридичну особу чи державу, а також і в інформаційно-комунікаційних системах (обладнання та програм), що вже є предметом кібербезпеки. Тому кібербезпека є складовою частиною інформаційної безпеки.

Кібербезпека є складним правовим явищем, у рамках якого функціонує механізм кіберзахисту, котрий є складною системою заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру. В. Бухарєв зауважує, що кібербезпека у вигляді об'єкта правової охорони безпосередньо стосується інтересів держави. Водночас, механізми її забезпечення не є однорідними і регулюються нормами різних галузей права [1, с. 19].

І. Діордіца вважає, по-перше, кібербезпека є самостійною (окремою) складовою національної безпеки; по-друге, кібербезпека вимагає розроблення і постійного удосконалення системних адміністративно-правових заходів. Варто погодитись з тим твердженням, що необхідно посилити роль держави в кіберпросторі, а також потрібно розробити чіткі механізми правового регулювання діяльності громадян в кіберпросторі [2, с. 37–38, 85–87].

Під поняттям «кіберпростір» Т. Білобров розуміє нове середовище для встановлення зв'язків суб'єктів правовідносин, який відрізняється від фізичного низкою специфічних ознак: 1) кіберпростір виникає в результаті функціонування інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем; 2) він не має чітко визначених територіальних меж та кордонів (не може вважатися територією); 3) глобальність; 4) не передбачає фізичного контакту суб'єктів правовідносин, які можуть бути і не ідентифікованими; 5) комунікація за допомогою цифрового зв'язку шляхом використання програмного та апаратного забезпечення на основі спеціальних протоколів» [3, с. 169].

Кіберпростір – це складне середовище взаємодії людей, програмного забезпечення та послуг у мережі Інтернет та функціонує за підтримки об'єднаних мереж і пристроїв інформаційних та комунікаційних технологій

(ICT, Information and communications technology). Однак є окремі питання безпеки, які не входять ні до сучасної інформаційної безпеки, ні до Інтернет-безпеки, ні до мережевої чи й ІСТ-безпеки, бо між цими видами безпеки є своєрідні прогалини, а також між організаціями та постачальниками послуг у кіберпросторі часто бракує тісних зв'язків. Це відбувається тому, що об'єднані мережі та пристрої в кіберпросторі мають багато власників, у кожного з яких свій власний бізнес та коло проблем, пов'язаних з експлуатацією та контролем. Кожна організація та постачальник послуг у кіберпросторі має свою точку зору на безпеку тих областей, у яких є незначний вхідний потік відомостей від іншої організації або постачальника, що призводить до фрагментації стану безпеки в кіберпросторі [4].

На міжнародному рівні в межах ООН права людини в кіберпросторі закріплюються, зокрема в Резолюції ГА ООН № 57/239 «Елементи для створення глобальної культури кібербезпеки» від 20.12.2002 р. У цьому акті закріплено 9 основних принципів культури кібербезпеки всіх учасників, які користуються інформаційними технологіями, починаючи від державних органів влади і аж до всіх інших індивідуальних споживачів. До цих принципів належить, зокрема, відповідальність, відповідно до якого усі суб'єкти, що здійснюють свою діяльність у кіберпросторі відповідальні за свої дії і безпеку їхніх об'єктів, дотримуючись всіх вимог з метою захисту інформаційних систем та зменшення ризиків пошкодження програмного забезпечення. Ця Резолюція ООН спрямована також і на громадянське суспільство, зокрема стосується кожної свідомої людини, яка вступає у правовідносини в кіберпросторі [5].

Крім того, була прийнята, зокрема, Резолюція ГА ООН № 58/199 «Створення глобальної культури кібербезпеки та захист критично важливих інформаційних інфраструктур» від 23 грудня 2003 року [6] говорить про необхідність доступу країн світу до інформаційно-комунікаційних технологій, щоб держави, які розвиваються, також могли їх використовуючи і для свого соціально-економічного розвитку.

Також була прийнята Резолюція ГА ООН № 68/167 «Право на приватність у цифрову епоху» (18 грудня 2013 року). У цьому документі зазначається, що користування новими комунікативними та інформаційними технологіями з одного боку полегшує державним органам збирати інформацію, а з іншого може обмежувати чи порушувати права людини. З метою забезпечення права на приватність, у цьому документі ООН закликає держави створити чи переглянути вже існуючі механізми нагляду за зв'язками та збору персональних даних [7]. На те, що прогрес у сфері інформаційних технологій може мати негативні наслідки для недоторканості, гідності і прав людини ООН звертала увагу ще у 1993 році у своїй Віденській декларації і програмі дій [8].

Інформаційна безпека в інтернеті була предметом обговорення і на 73 сесії ГА ООН. У Резолюції ГА ООН № 73/27 «Досягнення в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» від 5 грудня 2018 року [9] зазначено, що держави мають бути зацікавлені в припиненні конфліктів, які виникають при використанні інформаційно-комунікаційних технологій і мають співпрацювати між собою, а також з приватними суб'єктами, з метою створення надійний умов для використання інформаційно-комунікативних технологій, довіри між контрагентами та забезпечення безпеки в системі виробництва та збуту інформаційних товарів і надання послуг на цьому ринку. А 22 грудня 2018 року ООН у своїй Резолюції № 73/266 «Заохочення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки» закликала держави відповідально використовувати інформаційно-комунікаційні технології з метою усунення загроз в сфері інформаційної безпеки [10].

12 грудня 2019 році було прийнято Резолюцію ГА ООН № 74/28 «Посилення відповідальної поведінки держави в кіберпросторі в контексті міжнародної безпеки» [11]. Таку ж назву також має Резолюція ГА ООН № 75/32, яка була прийнята 7 грудня 2020 року [12]. В останній наголошується, що інформаційно-комунікаційні технології можуть використовуватися по різному – з одного боку можуть бути використані для забезпечення міжнародної безпеки та стабільності, а з іншого – для порушення цілісної інфраструктури держав чи у воєнній сфері. ГА ООН в цій резолюції наголошує на необхідності збереження вільного потоку інформацією та закликає держави забезпечити відкрите, надійне і безпечне інформаційно-комунікативне середовище, в тому числі запобігаючи можливим атакам.

Забезпечення прав людини у кіберпросторі також регулюється і на європейському рівні в межах Ради Європи та Європейського Союзу (далі – ЄС).

Держави-члени Ради Європи 23 листопада 2001 року прийняли Конвенцію про кіберзлочинність. Україна ратифікувала цю конвенцію Законом № 2824-IV від 7 вересня 2005 року [13]. У вказаному акті сформульовано принципи щодо здійснення заходів по боротьбі з кіберзлочинністю на національному і міжнародному рівні [14, с.107]. Конвенція спрямована на захист конфіденційності, цілісності комп'ютерних систем, мереж та даних і передбачає необхідність встановлення кримінальної відповідальності за їх порушення. У Конвенції про кіберзлочинність закріплено декілька категорій правопорушень, зокрема, правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ до цілої комп'ютерної системи чи її частини, нелегальне перехоплення комп'ютерних даних чи втручання у такі дані, пошкодження комп'ютерних систем) та правопорушення пов'язані з комп'ютерами (підробка комп'ютерних даних, шахрайство, пов'язане з втратою (знищенням) таких даних та втручання в функціонування комп'ютерних систем). Відповідно до ст. 19 Конвенції компетентні органи держави повинні мати можливість проводити обшук чи отримувати доступ до комп'ютерних систем, комп'ютених даних чи носія інформації з метою розкриття кіберзлочинів [15].

У преамбулі до Конвенції про кірезлочинність зазначено, що держави пам'ятають про право на захист особистої інформації, яке передбачене Конвенцією Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28 січня 1981 року. Ця Конвенція спрямована на захист недоторканості приватного життя у зв'язку з обробкою персональних даних особи, які автоматизовано збираються та обробляються [16]. Обов'язок держави чи організації забезпечити необхідний рівень захисту при передачі даних передбачений і в Додатковому протоколі до Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних» від 8 листопада 2001 року. Україна цю Конвенцію та Додатковий протокол до неї ратифікувала Законом України № 2438-VI від 6 липня 2010 року [17].

Будь-які заходи безпеки, спрямовані на захист Інтернет-користувачів від кіберзлочинності, повинні також відповідати міжнародним стандартам щодо права на приватне і сімейне життя та права на свободу вираження поглядів, які передбачені Конвенцією про захист прав людини та основоположних свобод від 4 листопада 1950 року та практикою Європейського суду з прав людини.

У зв'язку з розвитком електронних комунікацій та необхідністю захисту персональних даних питань виникає потреба у врегулюванні цих відносин і в країнах-членах ЄС. Право на захист особистих даних та свобода вираження поглядів та інформації закріплені в Хартії основних прав Європейського Союзу [18].

11 грудня 2018 року в межах ЄС була прийнята Директива Європейського Парламенту і Ради ЄС 2018/1972 «Про запровадження Європейського кодексу електронних комунікацій» з метою запровадити внутрішній ринок електронних комунікаційних мереж та послуг, що призведе, в тому числі і до їх безпеки. Відповідно до пункту 21 статті 2 цієї Директиви «безпека мереж і послуг» означає здатність електронних комунікаційних мереж і послуг протистояти, з певним рівнем впевненості, будь-яким діям, які підривають доступність, автентичність, цілісність або конфіденційність цих мереж і послуг, збережених, переданих або оброблених даних, або пов'язаних з ними послуг, що надаються або доступні через ці електронні комунікаційні мережі або послуги [19].

У 2004 році в ЄС було створено Європейське агенство з питань мережевої та інформаційної безпеки (European Union Agency for Network and Information Security), у повноваження якого входить надання рекомендацій з інформаційної та кібербезпеки, проведення експертизи з питань, що пов'язані з інформаційною мережею та безпекою на запити інституцій та держав-членів ЄС [20].

16 грудня 2020 року Єврокомісія прийняла Стратегію кібербезпеки ЄС у цифрове десятиліття, а 22 березня 2021 року Рада ЄС ухвалила резолюцію на підтримку цієї Стратегії з метою захисту громадян та бізнесу від кібератак та забезпечення безпечного кіберпростору. Для досягнення цієї мети зазначається необхідність створення мережі оперативних центрів з безпеки в межах ЄС, які будуть займатися прогнозуваннями, виявленням та протидією кібератак. Також в Стратегії звернено увагу на необхідність впровадження стандартів безпеки в інтернеті та розвиток надійного шифрування як засобу захисту прав суб'єктів та цифрової безпеки [21].

Отже, міжнародне співтовариство ініціативно реагувало на право людини на приватне життя, захист персональних даних та право на інформацій безпеку. Тому злочини у сфері кіберпростору були визнані серйозною проблемою для загального миру і безпеки. Багато держав тепер за допомогою механізмів міжнародного співробітництва в галузі права та безпеки взяли на себе зобов'язання ефективно боротися з кіберзлочинами та кібертероризмом, ретельно стежачи за тим, щоб технології, комунікації та ресурси не використовувалися для злочинів з метою, зокрема, викорінення можливості для поширення терористичної та екстремістської ідеології в інтернеті. Було досягнуто значного прогресу в розробці норм двостороннього і багатостороннього співробітництва в справі боротьби зі злочинами в сфері Інтернету [22].

Отже, регулювання кібербезпеки має глобальне значення і відбувається на міжнародному рівні. В Україні також є законодавство, яке регулює захист прав людини в сфері кіберпростору. Проте ще тема наступної статті. З вищезазначеного все ж випливає необхідність розробки та постійного удосконалення нормативно-правового регулювання кібербезпеки враховуючи міжнародні рекомендації та ратифіковані акти щоб адекватно запобігати загрозам, які існують в цій сфері. На міжнародному рівні фактично виробляються стандарти безпеки, які повинні дотримуватися на об'єктах критичної інфраструктури, а їх недотримання має означати можливість притягнення винних осіб до юридичної відповідальності.

ЛІТЕРАТУРА

1. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України. Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Суми : Університет сучасних знань ; Сумський державний університет, 2018. 221 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/70638/1/diss_Bukhariev.pdf (дата звернення: 15.05.2022).
2. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України. Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Запоріжжя : Запорізький національний університет, 2018. 521 с. URL: http://phd.znu.edu.ua/page//dis/07_2018/Diorditsa-pdf.pdf (дата звернення: 15.05.2022).
3. Білобров Т.В. Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України. Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ : НАВС, 2020. 209 с. URL: http://elar.naiau.kiev.ua/jspui/bitstream/123456789/17029/5/dys_bilobrovtv.pdf (дата звернення: 16.05.2022).
4. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT) від 27.12.2016. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128 (дата звернення: 16.05.2022).
5. Элементы для создания глобальной культуры кибербезопасности: резолюция Генеральной Ассамблеи ООН от 20.12.2002 № 57/239. *Офіційний сайт ВР України*. URL: https://zakon.rada.gov.ua/laws/show/995_b42#Text (дата звернення: 17.05.2022).
6. Creation of a global culture of cybersecurity and the protection of critical information infrastructures Resolution adopted by the General Assembly on 23 December 2003 № 58/199, United Nations. *Official site of the United Nations*. URL: https://undocs.org/en/A/RES/58/199 (date of application: 18.05.2022).
7. The right to privacy in the digital age: Resolution adopted by the General Assembly on 18 December 2013 № 68/167, United Nations. *Official site of the United Nations*. URL: https://undocs.org/en/A/RES/68/167 (date of application: 18.05.2022).
8. Венская декларация и Программа действий: принята на Всемирной конференции по правам человека в Вене 25.06.1993 г. *Офіційний сайт ВР України*. URL: https://zakon.rada.gov.ua/laws/show/995_504#Text (дата звернення: 20.05.2022).
9. Developments in the field of information and telecommunications in the context of international security: Resolution adopted by the General Assembly on 5 December 2018 № 73/27, United Nations. *Official site of the United Nations.* URL: https://undocs.org/en/A/RES/73/27 (date of application: 18.05.2022).
10. Advancing responsible State behaviour in cyberspace in the context of international security: Resolution adopted by the General Assembly on 22 December 2018 № 73/266, United Nations. *Official site of the United Nations*. URL: https://undocs.org/en/A/RES/73/266 (date of application: 19.05.2022).
11. Advancing responsible State behaviour in cyberspace in the context of international security: Resolution adopted by the General Assembly on 12 December 2019 № 74/28, United Nations. *Official site of the United Nations.* URL: https://undocs.org/en/A/RES/74/28 (date of application: 20.05.2022).
12. Advancing responsible State behaviour in cyberspace in the context of international security: Resolution adopted by the General Assembly on 7 December 2020 № 75/32, United Nations. *Official site of the United Nations.* URL: https://undocs.org/en/A/RES/75/32 (date of application: 20.05.2022).
13. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV. *Офіційний сайт ВР України*. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення: 21.05.2022).
14. Бєлявцева В.В. До питання застосування правових режимів забезпечення кібербезпеки в Україні. *Інформація і право*. 2020, № 4(35). С.106-112. URL: http://il.ippi.org.ua/article/view/221235 (дата звернення: 21.05.2022).
15. Конвенція про кіберзлочинність: Рада Європи; Конвенція, Міжнародний документ від 23.11.2001. *Офіційний сайт ВР України*. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 22.05.2022).
16. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Рада Європи; Конвенція, Міжнародний документ від 28.01.1981. *Офіційний сайт ВР України*. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 22.05.2022).

17. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних. *Офіційний сайт ВР України*. URL: https://zakon.rada.gov.ua/laws/show/2438-17#Text (дата звернення: 22.05.2022).

18. Хартия основных прав Европейского Союза: междунар. док. от 07.12.2000. *Офіційний сайт ВР України*. URL: http://zakon2.rada.gov.ua/laws/show/994_524 (дата звернення: 23.05.2022).

19. Директива Європейського Парламенту і Ради (ЄС) 2018/1972 про запровадження Європейського кодексу електронних комунікацій від 11.12.2018. *Офіційний сайт ВР України*. URL: https://zakon.rada.gov.ua/laws/show/984_013-18#Text (дата звернення: 23.05.2022).

20. Бойко В.Д., Василенко М.Д., Кухаренко С.В. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення. *Інформаційна безпека людини, суспільства, держави.* 2019. № 3 (27). С. 49-56. URL: http://nbuv.gov.ua/UJRN/iblsd_2019_3_8 (дата звернення: 24.05.2022).

21. Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy: European Council, Council of the European Union, 22 March 2021. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/ (date of application: 24.05.2022).

22. Report on World Internet Development 2016 of World Internet Conference «Innovation-driven Internet Development for the Benefit of All – Building a Community of Common Future in Cyberspace». URL: http://www.wuzhenwic.org/2016-11/18/c_61834.htm (date of application: 24.05.2022).