УДК 342.7:004.738
DOI https://doi.org/10.24144/2788-6018.2025.06.1.26

ПРАВО ЛЮДИНИ НА КІБЕРБЕЗПЕКУ: СУТНІСНІ ХАРАКТЕРИСТИКИ ТА ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ

Марушка М.Т.,
студентка,
юридичний факультет
ДВНЗ «Ужгородський національний університет»
ORCID: 0009-0006-0631-4707
e-mail: marushka.melinda@student.uzhnu.edu.ua

Геревич М.О.,
доктор філософії, доцент кафедри теорії
та історії держави і права
ДВНЗ «Ужгородський національний університет»
ORCID: 0000-0002-0842-2828

Марушка М.Т., Геревич М.О. Право людини на кібербезпеку: сутнісні характеристики та проблеми забезпечення.

Стаття присвячена комплексному аналізу права людини на кібербезпеку як одного з фундаментальних прав четвертого покоління та його місця в системі прав людини. Авторами розглядаються сутнісні характеристики цього права у контексті сучасного цифрового суспільства та актуальних викликів, які виникають унаслідок розвитку інформаційно-комунікаційних технологій.

Авторами проведено детальний аналіз різноманітних видів кіберзагроз на індивідуальному рівні, зокрема кібершахрайства, фішингових атак, зломів акаунтів у соціальних мережах та встановлення шкідливого програмного забезпечення, з наведенням конкретних судових прикладів.

Значну частину статті присвячено дослідженню кібератак державного масштабу та їх впливу на національну безпеку України в умовах повномасштабного вторгнення. Представлено статистичні дані про зростання кількості зареєстрованих кіберінцидентів, детально проаналізовано категорії подій інформаційної безпеки, розглянуто конкретні приклади масштабних атак на критичну інфраструктуру (атака на Viasat, кібератака на мережу «Київстар», атаки на Єдині державні реєстри України). Авторами обґрунтовано розуміння кібербезпеки як важливої складової національної безпеки держави.

У роботі аналізуються механізми забезпечення права на кібербезпеку з боку держави, зокрема діяльність органів, відповідальних за кібербезпеку, та прийняті нормативно-правові акти. Одночасно акцентується на ролі самої особи у забезпеченні власної кібербезпеки, виокремлюються практичні заходи запобігання кіберзагрозам. Розглядаються конституційні гарантії права на кібербезпеку, закріплені у статтях 31 та 32 Конституції України.

Особлива увага приділяється міжнародному аспекту забезпечення кібербезпеки, зокрема ролі Конвенції про кіберзлочинність, прийнятої Радою Європи у Будапешті 2001 року. Авторами обґрунтовується необхідність міжнародної співпраці між державами для вирішення проблем кіберзлочинності та захисту прав людини у цифровому просторі.

Ключові слова: кібербезпека, права людини, національна безпека, кіберзлочини, цифровий простір.

Marushka M.T., Gerevych M.O. The human right to cybersecurity: essential characteristics and problems of ensuring.

The article is devoted to a comprehensive analysis of the human right to cybersecurity as one of the fundamental rights of the fourth generation and its place in the system of human rights. The authors consider the essential characteristics of this right in the context of a modern digital society and current challenges that arise as a result of the development of information and communication technologies.

The authors conducted a detailed analysis of various types of cyber threats at the individual level, in particular, cyber fraud, phishing attacks, hacking of accounts in social networks and the installation of malicious software, with specific judicial examples.

A significant part of the article is devoted to the study of state-scale cyber attacks and their impact on the national security of Ukraine in the context of a full-scale invasion. Statistical data on the growth in the number of registered cyber incidents are presented, categories of information security events

are analyzed in detail, specific examples of large-scale attacks on critical infrastructure are considered (attack on Viasat, cyberattack on the Kyivstar network, attacks on the Unified State Registers of Ukraine). The authors substantiate the understanding of cybersecurity as an important component of the state's national security.

The paper analyzes the mechanisms for ensuring the right to cybersecurity by the state, in particular the activities of bodies responsible for cybersecurity, and adopted regulatory legal acts. At the same time, the role of the individual in ensuring his or her own cybersecurity is emphasized, and practical measures to prevent cyber threats are highlighted. The constitutional guarantees of the right to cybersecurity, enshrined in Articles 31 and 32 of the Constitution of Ukraine, are considered.

Special attention is paid to the international aspect of ensuring cybersecurity, in particular the role of the Convention on Cybercrime, adopted by the Council of Europe in Budapest in 2001. The authors substantiate the need for international cooperation between states to address the problems of cybercrime and protect human rights in the digital space.

Key words: cybersecurity, human rights, national security, cybercrime, digital space.

Постановка проблеми. Сьогодні ми живемо у світі цифрових технологій, які постійно удосконалюються. З розвитком сучасних технологій постає питання врегулювання нових правовідносин, які виникають у суспільстві. Поруч із новими перспективами зростають і нові загрози у цифровому середовищі. Постає необхідність вміння попередження і виявлення таких загроз та знаходження методів боротьби з ними. В зв'язку із масштабністю кіберпростору, його можна вважати недостатньо дослідженим.

Зараз відбувається регламентація основоположних засад щодо кіберпростору і безпеки його використання. Оскільки, кіберпростір може не обмежуватись територіальними межами країн є необхідною співпраця між державами для забезпечення єдиного безпечного кіберпростору. Важливо, щоб правове регулювання кібербезпеки не відставало від розвитку цифрових технологій. Тільки так можна забезпечити належну захищеність осіб від кіберзагроз.

Актуальним на сьогодні є забезпечення права людини на кібербезпеку, оскільки кожен день проведений в цифровому середовищі несе нові загрози і потребує захисту осіб. Проводячи час у кіберпросторі, користувач може натрапити на небезпеку. Проте, буває і таке, що порушення у цій сфері трапляються не з вини користувача і загрожує національній безпеці.

Стан дослідження. Дослідження проблематики забезпечення кібербезпеки з теоретичної і практичної точки зору у своїх наукових працях розвивали М.І. Давидович, А.О. Довгополов, Є.Ю. Колосовський, М.М. Корчук, Е.М. Круць, Я.П. Мазур, С.Р. Микитчин, І.М. Сопілко, О.О. Тихомиров, Ю. Хобі, Р.А. Яремко. Результати їхніх досліджень дають нам змогу аналізувати ступінь забезпеченості безпеки у кіберпросторі та гарантування права людини на кібербезпеку. В зв'язку з постійним розвитком цифрових технологій випливає, що дане питання потребує більш детального дослідження.

Метою статті є аналіз права людини на кібербезпеку, стан забезпеченості цього права, виявлення загроз, які виникають у кіберпросторі та визначення кібербезпеки як одного з елементів національної безпеки.

Виклад основних положень. На початку розгляду теми, необхідно визначити ключові поняття даного дослідження. Одним з таких термінів виступає «кібербезпека». Відповідно до формулювання терміну, яке зазначено у Законі України «Про основні засади забезпечення кібербезпеки України», кібербезпека – передбачає захищеність важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1, ст. 1].

Часто кібербезпеку ототожнюють з інформаційною безпекою, проте ці два поняття є різними. Інформаційна безпека являє собою стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди, що виникає внаслідок неповноти, невчасності та невірогідності інформації, яка використовується; негативного інформаційного впливу; негативних наслідків застосування інформаційних технологій; несанкціонованого розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [2, п. 13].

Розмежовуючи ці поняття, можна сказати, що кібербезпека є складовою частиною інформаційної безпеки і стосується тільки цифрового середовища. Вона спрямована на захист прав і свобод людини під час використання кіберпростору. Вже інформаційна безпека є більш ширшим поняттям і застосовується не тільки в цифровому просторі, але й в інших сферах, спираючись саме на конфіденційність та захисту інформації й доступу до неї [3, с. 43].

Розглядаючи кібербезпеку більш широко, можна відмітити певні її особливості. Однією з них є те, що вона спрямована на захист комп'ютерних систем від кібератак та унеможливлення витоку даних, які зберігаються у цифровому середовищі. Також кібербезпека полягає у захисті персональних даних від несанкціонованого доступу до них. Варто відмітити, що кібербезпека включає в себе декілька елементів, зокрема це безпека додатків, безпека даних, хмарна безпека, безпека критично важливої інфраструктури, планування аварійного відновлення та навчання кінцевих користувачів [4, с. 111].

Право людини на кібербезпеку можна віднести до четвертого покоління прав людини, а саме до типу інформаційних прав. Поява цього покоління прав людини пов'язана зі стрімким розвитком технологій. Відповідно, з розвитком нових правовідносин повинно відбуватися швидке реагування на такі зміни –вчасна регламентація прав особи та їх гарантування державою.

Це право у сучасному світі вважається невід'ємним та невідчужуваним правом людини. Проте, в сучасних реаліях, його досить важко забезпечити. Звичайно, держава робить для гарантування і забезпечення права на кібербезпеку все необхідне: регламентує норми кібербезпеки в національному законодавстві та передбачає відповідальність за кіберзлочини, забезпечує політику протидії кіберзагрозам, захищає інформаційні системи та конфіденційну інформацію, утворює і скеровує роботу відповідних органів, які б забезпечували це право.

До органів, які забезпечують кібербезпеку належать Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України, Генеральний штаб Збройних сил України. Також Україна має армію IT-фахівців, які захищають інтереси в цифровому середовищі та здійснюють зустрічне атакування серверів країни-агресора [5, с. 13; 6, с. 404].

Проте, забезпечення кібербезпеки залежить не тільки від самої держави, але і від кожної особи. Оскільки правовідносини, які виникають у кіберсфері є порівняно новими і їх масштаб величезний, вслідкувати за всім, що відбувається у цьому просторі, на сьогодні дається досить важко. Варто навести кілька аргументів, чому пильність особи є важливою складовою кібербезпеки.

По-перше, найчастіше кіберзлочини стаються через бажання осіб «зловити» вигідну пропозицію і небажання перевірити надану інформацію. Тому, до злочинів у кіберсфері можна віднести й кібершахрайство. Воно здійснюється щодо індивідуальних користувачів. Такий вид кіберзлочину тягне за собою майнові збитки для користувачів. Найбільш поширюваним видом кібершахрайства є покупки в мережі Інтернет. Часто особи намагаються знайти вигідні пропозиції, сплачуючи кошти шахраям. Таке явище може бути поширеним через недостатній рівень обізнаності та проінформованості користувачів про можливі загрози у кіберпросторі, оскільки особи не перевіряють інформацію про продавця. Цей аспект залишається недостатньо захищеним у кіберпросторі, оскільки неможливо відстежувати всіх користувачів, які здійснюють діяльність в Інтернеті. Тому без пильності осіб в цьому плані не обійтись.

По-друге, останнім часом поширюється такий вид шахрайства як злом акаунтів користувачів у соціальних мережах та прохання від імені користувача грошей у підписників. Багато людей довіряють, і пересилають кошти на картку шахраїв, не перевіривши, чи дійсно знайомий користувач потребує допомоги. В таких випадках варто написати на інший месенджер або перетелефонувати для підтвердження такої інформації. Для поновлення порушеного права особи мають можливість звернутися до компетентних органів. Підслідність таких справ належить кіберполіції. Проте, в таких випадках варто проявити користувачеві обачність для можливості недопуску зламу акаунту. Зокрема, це може бути встановлений надійний пароль, не пов'язаний із відомими датами, але з використанням різних символів. Також варто встановлювати двофакторну автентифікацію при вході в акаунт. Важливим елементом є також заборона переходу через підозрілі посилання, оскільки для можливості взлому акаунту шахраї найчастіше пропонують такий варіант.

З цього випливає ще одна загроза в умовах цифрової трансформації –фішингові посилання. Тобто, це певне шкідливе посилання, створене шахраями, через які вони можуть зламати акаунт у соціальних мережах, отримати доступ до персональної інформації та банківських карток. Досить часто користувачі переходять за різними посиланнями, не перевіряючи назву цих посилань, користувача, який їх надіслав або сповіщення безпеки. Через свою довірливість вони часто водять паролі банківських карток чи іншу особисту інформацію. Також цей вид шахрайства може бути застосований за допомогою телефонних дзвінків, шляхом розпитування номерів банківських карток та їх паролів.

По-третє, надаючи свої персональні дані в цифровому середовищі особа повинна детально ознайомитися яким чином і куди передаватимуться її дані, хто буде їх володільцем. Проте, досить часто на цей пункт особи не звертають уваги через небажання витрачати час на прочитання умов політики конфіденційності. Або ж особа встановлює мобільний застосунок з шкідливим програмним

забезпеченням, тим самим роблячи свій пристрій вразливим та надаючи доступ до конфіденційної інформації.

Досить цікавий приклад шахрайства можна навести із судової справи № 554/10000/16-к від 2016 року. Шахрайство здійснювалося за допомогою шкідливої комп'ютерної троянської програми «URLzone», або так званого банківського трояна. Після встановлення програми на автоматизовану електронно-обчислювальну машину (комп'ютер), шахраї мали змогу отримати банківські дані осіб. Після цього цим користувачам надходили повідомлення про помилкове зарахування грошових коштів та прохання їх повернення. Особи довіряли, і переправляли на рахунок шахраїв власні кошти [7].

Ці приклади показують сторону незахищеності кіберпростору. З цього випливає, що кібербезпеку повинна забезпечувати не тільки держава та інші установи, але дуже багато чого залежить саме від особи. Тому зважаючи на вищесказане, можна виокремити такі ключові заходи із запобігання кіберзагроз: використання багатофакторної автентифікації; створення надійного паролю, з використанням різних символів; заборона переходу за підозрілими посиланнями; заборона передачі персональних даних незнайомим особам; перевірка достовірності інформації; вчасне оновлення програмного забезпечення; використання антивірусного програмного забезпечення [8].

Право на кібербезпеку не варто розглядати тільки як захист від фішингових посилань, зламу акаунтів чи інших втручань в приватне життя, які не мають державного масштабу. Право людини на кібербезпеку варто розглядати і в контексті всієї національної безпеки, коли відбувається кібератака на державні реєстри чи інші державні сервери. Адже цілями кіберзлочинів може поставати не тільки бажання збагатитися, але й бажання паралізувати роботу установ та організацій та отримати доступ до конфіденційної інформації.

Кібербезпека є важливою складовою національної безпеки держави. Особливо це помітно в умовах воєнного стану, оскільки війна відбувається не тільки на суші, морі та повітрі, але й в кіберпросторі. Він вважається новим середовищем для злочинних дій в сфері несанкціонованого доступу до конфіденційної інформації. З початку повномасштабного вторгнення кількість зареєстрованих випадків кіберінцидентів збільшилась вдвічі. Число кібератак, на системи, які мають високий рівень критичності з боку росії, зросли в чотири рази [6].

Варто навести приклад кібератаки, яка сталась у день повномасштабного вторгнення. Кібернетична атака була здійснена на супутниковий доступ до Інтернету компанії Viasat. Проте, як було з'ясовано пізніше, метою цієї атаки був не доступ до даних, а переривання обслуговування. Зокрема, країна-агресор хотіла не тільки унеможливити доступ цивільного населення до Інтернету та достовірної інформації, але й порушити роботу управління та українського командування під час вторгнення. Це ще раз підтверджує те, що війна між Україною і росією має гібридний характер. Проте, впливу цієї хакерської атаки зазнала не тільки Україна, але і Європа [9].

Ще одна масштабна хакерська атака з боку росії відбулася 12 грудня 2023 року на мережу мобільного оператора «Київстар». Внаслідок чого користувачі не мали доступу до зв'язку та Інтернету, а також інші фінансові компанії не могли надати певні послуги. Ця кібератака мала низку загроз, зокрема несанкціонований доступ до персональної інформації користувачів, отримання місцезнаходження телефонів, перехоплення повідомлень та доступ до акаунтів Telegram. Ця атака повністю порушила право осіб на приватність та повагу до особистого життя [10].

У контексті цього дослідження не можна не згадати про масштабну кібератаку на Єдині державні реєстри України, зокрема на реєстри Міністерства юстиції України, яку здійснили хакери країни-агресора 19 грудня 2024 року. Залишається непідтвердженою інформація про витік персональних даних. У разі якщо персональні дані були отримані російськими хакерами, то це може негативно вплинути на подальший розвиток подій. Зокрема, через доступ до персональних даних, може відбуватись пошук колаборантів та вербування осіб, здійснюватись на них вплив та тиск, вестись інформаційно-психологічна операція [11].

Звичайно, кількість кібератак в Україні є значною. Можна зробити висновок, що під час повномасштабного вторгнення численні атаки спрямовані саме на припинення роботи певних ресурсів, зокрема серверів, або погіршення їх діяльності (DDoS) [9].

Якщо переглянути звіти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації до початку повномасштабного вторгнення та після нього, то можна помітити суттєві зміни зростання кількості кібератак. На основі аналізу цих даних пропонуємо розглянути таблицю.

Таблиця 1 – Кількість кібератак до і після повномасштабного вторгнення

	Зареєстровано кіберінцидентів	Детектовано підозрілих подій ІБ	Опрацьовано критичних подій ІБ
2021	147	41 млн	160 тис.
2022	415 (на 2.8% більше, ніж у 2021 р.)	181 млн	179 тис.
2023	1105 (на 62.5% більше, ніж у 2022 р.)	133 млн	148 тис.
2024	1042	2.95 млн (суттєва різниця через модернізацію систем)	28 тис.

Джерело: складено авторами на основі [8, 12, 13, 14]

Відповідно до звіту за 2022 рік Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації кількість критичних подій, джерелом яких є IP-адреси росії з початку повномасштабного вторгнення зросла на 26% [13].

Також між цими звітами можна помітити різницю. З кожним роком він вдосконалюється і містить більше відомостей, ніж попередній звіт. До прикладу, звіт за 2024 рік містить відомості про кіберінциденти за секторами. І з цього можна сказати, що кібератак зазнали 5 оборонних об'єктів, 65 урядових та 1 енергетичний об'єкт [8].

З початком повномасштабного вторгнення відбулись зміни у категоріях подій інформаційної безпеки. Найбільш поширеним методом кібератак стало застосування шкідливих програмних кодів. Це продемонструє таблиця.

Таблиця 2 – категорії подій інформаційної безпеки до і після повномасштабного вторгнення

	2021	2022	2023	2024
Шкідливий програмний код	28%	↑ 18.3 рази (прибл. 88%)	↑ 36.2 рази (прибл. 91%)	58.8%
Збір інформації зловмисником	18%	↑ 2.2 рази (прибл. 5 %)	↑ 43.8 рази (прибл. 6%)	12,1%
Спроби втручання	1%	прибл. 3%	прибл. 1.5%	17,6%
Інше	53%	прибл. 4%	прибл. 1.5%	11,5%

Джерело: складено авторами на основі [8, 12, 13, 14]

Варто зазначити, що під час повномасштабного вторгнення кібератаки спрямовані на сайти державного управління, ЗМІ, інформаційно-комунікаційні системи, фінансові організації. Така спрямованість пояснюється тим, що країна-агресор прагне отримати конфіденційну інформацію, поширити дезінформацію у суспільстві та збільшити його недовіру.

Одним з видів кіберзлочинів, який має на меті поширення неправдивої інформації – виступає підробка відео. Зокрема, найчастіше відбувається розповсюдження відео з публічною особою, яка розголошує вигідні для кіберзлочинців відомості. Такі дії відбуваються для поширення дезінформації та паніки у суспільстві. Це є один з прийомів інформаційно-психологічної операції (ІПСО). Цей вид правопорушення у кіберсфері набув великого поширення, після повномасштабного вторгнення, проте, він мав місце й раніше. Звідси постає необхідність навчання осіб вчасно виявляти такі фейки та не поширювати їх серед інших користувачів [6, С. 404].

Держава здійснює низку заходів, щоб забезпечення права людини на кібербезпеку. Одним з таких виступає правова регламентація, а саме прийняття законодавчих актів, які б регулювали стандарти кібербезпеки. Важливими прийнятими нормативно-правовими актами щодо кібербезпеки є Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про захист персональних даних», Закон України «Про захист інформації в інформаційно телекомунікаційних системах» [5, с. 12-13].

Сьогодні, в умовах війни, у законодавство, яке стосується кібербезпеки, вносяться постійні зміни та усуваються прогалини. Нові норми стосуються притягання винних до відповідальності за кіберзлочини та їх виявлення і розслідування. Варто розуміти, що кіберзлочини загрожують національній безпеці. Тому, відповідальність за вчинення кіберзлочину настає відповідно до кримінального законодавства. Отже, внесені доповнення стосуються кримінального законодавства.

Зокрема, було внесено зміни до Кримінального процесуального кодексу України, які стосуються підвищення ефективності досудового розслідування кіберзлочинів. Також до Кримінального кодексу України було внесено зміни щодо підвищення боротьби з кіберзлочинністю в умовах воєнного стану. Проте, у Кримінальному кодексі України не зустрічаються поняття «кіберзлочину» та «кібербезпеки». Це свідчить про те, що поки поняття «кіберзлочин» виконує інтерпретаційну функцію і не застосовується самостійно в процесуальних документах. Натомість, це поняття виражається як несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних, електронних комунікаційних мереж [5, с. 14; 15, с. 302].

Звідси випливає, що кіберзлочин включає також несанкціоноване втручання в комунікаційні мережі. Виходячи з дефініції даного поняття, можна сказати, що сюди відносять телефонні розмови, повідомлення інформації або обмін даними через певні месенджери. А отже, отримання інформації шляхом такого втручання без дозволу власника або у випадках, які не передбачені законом прямо порушує статтю 31 Конституції України. Вона вказує на те, що кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Тому, можна сказати, що ця норма Основного Закону певним чином стосується права людини на кібербезпеку [16, ст. 31].

Під час різноманітних хакерських атак національного рівня відбувається пряме несанкціоноване втручання в приватне життя особи. Відповідно до статті 32 Конституції України «не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». До конфіденційної інформації відноситься й та інформація, яка зберігається у цифровому форматі [16, ст. 32].

Розуміючи, що розвиток цифрових технологій зумовлює виникнення нових ризиків, держави спільними зусиллями намагаються захистити права людини шляхом регламентації основоположних засад. Важливим кроком для посилення безпеки осіб у кіберпросторі стало прийняття Радою Європи у Будапешті 2001 року Конвенції про кіберзлочинність. До цієї Конвенції приєдналася й Україна. Основною її метою виступає захист суспільства від кіберзлочинності шляхом створення відповідного законодавства. Важливим є те, що Конвенція прийнята зважаючи на право про захист особистої інформації, забезпечуючи баланс між правоохоронними інтересами і повагою до основних прав людини [17].

З кожним днем перед різними державами світу постають нові виклики щодо захисту прав людини. І тільки у співпраці між собою ці виклики можливо вирішити. Конвенція забезпечує створення єдиного правового підходу між державами та зміцнення міжнародного співробітництва для розслідування кіберзлочинів та переслідування їх суб'єктів [18, с. 390].

Метою статті є аналіз права людини на кібербезпеку, стан забезпеченості цього права, виявлення загроз, які виникають у кіберпросторі та визначення кібербезпеки як одного з елементів національної безпеки.

Висновки. На сьогоднішній день розвиток цифрових технологій зростає з геометричною прогресією, проте разом із тим в найближчі 5-10 років інформаційний кіберпростір теж буде зростати з геометричною прогресією. Вже сьогодні можна помітити, що кіберпростір зустрічається в усіх сферах, зокрема як в функціонування державних установ, так і в особистому житті. Саме тому виникає необхідність визначення ролі права людини на кібербезпеку. У сучасному суспільстві воно вважається невідчужуваним, а його поява є реакцією держави на стрімкий розвиток нових правовідносин. Це право охоплює забезпечення безпеки у кіберпросторі, захист персональних даних, які розміщуються на електронних носіях інформації чи розташовані в електронних базах даних, запобігання проявів кіберзлочинів та гарантування права осіб на безпечний доступ до інформації.

Визначаючи практично спрямовані аспекти права на кібербезпеку, необхідно відмітити, що у сучасному суспільстві постає необхідність забезпечення безпечного кіберпростору. Зараз, держава здійснює різні заходи для гарантування кібербезпеки, але багато що залежить і від самих осіб. Найчастіше різноманітні прояви кіберзлочинів виникають саме із необачності особи. Проте, також можна помітити, що в самій Конституції України право на кібербезпеку не є прямо закріпленим, а тільки випливає із інших закріплених прав. В зв'язку з цим, після завершення воєнного стану, питання винесення права людини на особистий кіберпростір та кібербезпеку як окремої статті Основного Закону буде розглядатися одним з перших.

Однією з важливих складових гарантування цього права є своєчасне виявлення та усунення загроз, які виникають у кіберпросторі. При цьому виявлення можливої кіберзагрози повинно відбуватися ще до моменту несанкціонованого втручання в кіберпростір. Оскільки, зі зрозумілих причин, якщо таке втручання відбулося і понесло за собою негативні наслідки, то право на кібербезпеку є вже порушеним і потребує відновлення.

Проаналізувавши даний аспект, можна беззаперечно сказати, що порушення права на кібербезпеку однієї людини тягне за собою більш масштабні наслідки. Це пояснюється тим, що кібербезпека є одним з структурних елементів національної безпеки. Особливо це помітно в умовах ведення воєнних дій. Оскільки саме кіберпростір стає ще одним напрямком для завдання шкоди встановленому у суспільстві порядку, порушення відчуття захищеності та сприяє поширенню недовіри серед населення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 року № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
2. Про Основні засади розвитку інформаційного суспільства в Україні в 2007-2015 роки: Закон України від 09.01.2007 року № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text.
3. Хобі Ю. Право людини на кібербезпеку: проблеми визначення та гарантування. *Юридичний вісник.* 2020. № 2. С. 37–43. URL: https://dspace.onua.edu.ua/items/c192f469-04d2-453f-ab8d-22cfb09cbafb .
4. Сопілко І.М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник.* 2021. № 2 (59). С. 110–115. URL: https://er.nau.edu.ua/server/api/core/bitstreams/52e06a96-8b60-4c8b-bffa-8f9b8f9b10fd/content
5. Мазур Я.П. Правові основи регламентації кібербезпеки. *Науковий вісник Ужгородського Національного Університету.* 2024. Вип. 85: ч. 3. С. 11–15. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/3-2.pdf.
6. Колосовський Є.Ю., Круць Е.М. Сучасний стан кібербезпеки України в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2023. № 12. С. 402–405. URL: http://lsej.org.ua/12_2023/100.pdf.
7. Апеляційний суд Полтавської області, 06 грудня 2016 № 554/10000/16-к (Україна). URL: https://reyestr.court.gov.ua/Review/63231531
8. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації. Річний звіт системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2024 рік. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006.
9. Кібервиміри збройного конфлікту в Україні. Квартальний аналітичний звіт з липня по вересень 2023 року. Cyber Place Institute. URL: https://cyberconflicts.cyberpeaceinstitute.org/report.
10. Бутурлим О. Хакери мали доступ до системи «Київстар» задовго до масштабної атаки: деталі від СБУ. 2024. URL: https://www.unian.ua/techno/ataka-na-kijivstar-v-sbu-rozpovili-koli-hakeri-otrimali-dostup-do-sistemi-12501375.html.
11. Куришко Д. Реєстри відновили. Які наслідки кібератаки для України. 2025. URL: https://www.bbc.com/ukrainian/articles/c5ye75y8415o.
12. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації. Звіт системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2021 рік. URL: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf.
13. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2022 рік. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf.
14. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2023 рік. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a.
15. Тихомиров О.О. Інформаційні права людини: теоретико-правова концептуалізація: дис. … д-ра юрид. наук: 12.00.01 / Національна академія Служби безпеки України. Київ, 2024. 530 с. URL: https://ippi.org.ua/sites/default/files/disertaciya_tihomirov.pdf.

16. Конституція України від 28.06.1996 року № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
17. Конвенція про кібербезпеку: Конвенція від 23.11.2001 року. № 994_789. *Відомості Верховної Ради України*. 2006. № 5-6. Ст. 71. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.
18. Давидович М.І., Микитчин С.Р., Корчук М.М., Довгополов А.О., Яремко Р.А. Права людини в епоху діджиталізації: виклики та перспективи. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2023. Вип. 36. С. 386–392. URL: https://nzlubp.org.ua/index.php/journal/article/view/1317/1142.
19. Бєлова М.В., Бєлов Д.М. Імплементація штучного інтелекту в досудове розслідування кримінальних справ: міжнародний досвід**.** *Аналітично-порівняльне правознавство*. № 2. 2023. С. 448-454. URL: https://app-journal.in.ua/wp-content/uploads/2023/05/80.pdf.