УДК 343.1
DOI 10.32755/sjlaw.2025.02.098

Селецький О. В.,
кандидат юридичних наук, доцент, декан юридичного факультету,
Національний університет «Чернігівська політехніка»,
м. Чернігів, Україна
ORCID: 0000-0002-8291-9736;
Костюченко Н. Д.,
студентка І курсу магістратури юридичного факультету,
Національний університет «Чернігівська політехніка»,
м. Чернігів, Україна
ORCID: 0009-0005-3087-0191

ПОНЯТТЯ ТА ЗМІСТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У статті проаналізовано поняття та зміст інформаційної безпеки, спираючись на нормативно-правові акти і доктринальні підходи. Розглянуто основні аспекти, що визначають інформаційну безпеку в сучасному суспільстві, а також виявлено ключові елементи, які впливають на її формування та розвиток. Визначено роль інформаційної безпеки у структурі національної безпеки. Наголошено на важливості забезпечення інформаційної безпеки в умовах повномасштабного вторгнення російської федерації.

Ключові слова: *інформаційна безпека, національна безпека, кібербезпека, захист інформації, інформаційні загрози.*

Постановка проблеми. Інформаційна безпека в сучасному глобалізованому світі набуває статусу одного з фундаментальних компонентів національної безпеки держави. В умовах стрімкого розвитку інформаційно-комунікаційних технологій і переходу до інформаційного суспільства захист інформаційного простору, критичної інформаційної інфраструктури та інформаційного суверенітету стає пріоритетним завданням державної політики.

Інформаційний простір сьогодні перетворився на арену геополітичного протистояння, де інформаційні впливи, кібератаки та дезінформація використовуються як інструменти гібридної війни. Ця тенденція підкреслює необхідність комплексного підходу до забезпечення інформаційної безпеки як невід'ємного елемента системи національної безпеки.

Концептуальне осмислення феномена інформаційної безпеки та її ролі у структурі національної безпеки потребує глибо-

кого аналізу її сутнісних характеристик, нормативно-правових засад та інституційних механізмів забезпечення. Розкриття взаємозв'язку між інформаційною та національною безпекою дозволяє виробити ефективні підходи до протидії сучасним викликам та загрозам інформаційного характеру.

Аналіз останніх досліджень і публікацій. Важливий внесок у наукове вивчення питання інформаційної безпеки зробили такі дослідники, як О. П. Баранов, О. Г. Боднарчук, О. І. Боднарчук, І. О. Валюшко, А. В. Гарбінська-Руденко, М. В. Глух, В. І. Гурковський, В. П. Кононенко, А. Ю. Нашинець-Наумова та інші.

Мета статті полягає в теоретико-правовому дослідженні поняття та змісту інформаційної безпеки як складової національної безпеки.

Виклад основного матеріалу. Варто одразу наголосити, що на рівні окремого законодавчого акта термін «інформаційна безпека» не визначений. У Конституції України та інших законах України цей термін неодноразово згадується, але його сутність не розкривається.

Натомість у Стратегії інформаційної безпеки, що затверджена Указом Президента України від 28 грудня 2021 року № 685/2021, інформаційна безпека України трактується як складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання і поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [1].

Також інформаційна безпека згадувалась у ст. 2 проєкту Концепції інформаційної безпеки України як стан захищеності життєво важливих інтересів людини і громадянина, суспільства

і держави, за якого можна запобігти завданню шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив і умисне спричинення негативних наслідків застосування інформаційних технологій [2].

Гурковський В. І. визначає це поняття як суспільні відносини, пов'язані із захищеністю життєво важливих інтересів людини і громадянина, суспільства та держави від реальних і потенційних загроз в інформаційному просторі, що є необхідною умовою збереження і примноження духовних і матеріальних цінностей державотворчої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантування, охорони, захисту і відстоювання її національних інтересів [3, с. 74].

Своєю чергою О. П. Баранов розглядає інформаційну безпеку як стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації та несанкціоноване поширення і використання інформації, а також через негативний інформаційний вплив і негативні наслідки функціонування інформаційних технологій [4, с. 60–62].

Таким чином, можна узагальнити, що інформаційна безпека – це стан захищеності інформаційного простору, що забезпечує захист інтересів особи, суспільства і держави від інформаційних загроз, цілісність та достовірність інформації, а також належне функціонування інформаційної інфраструктури.

Важливим аспектом забезпечення інформаційної безпеки в Україні є розвиток нормативно-правової бази. Чинне законодавство потребує систематичного оновлення та гармонізації з сучасними викликами й загрозами.

Так, відповідно до ст. 17 Конституції України забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу [5]. Це конститу-

ційне положення підкреслює особливу значущість інформаційної безпеки в системі національних пріоритетів та визначає її як фундаментальну цінність, що потребує захисту на найвищому державному рівні.

Важливість забезпечення інформаційної безпеки визначена й у Законі України «Про національну безпеку України». Зокрема, в частині 4 статті 3 цього Закону зазначено, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями [6].

Забезпечення інформаційної безпеки України визначено одним з основних напрямів державної інформаційної політики згідно з частиною 1 статті 3 Закону України «Про інформацію» [7].

Значну роль у становленні нормативно-правового регулювання інформаційної безпеки в Україні відіграє Кримінальний кодекс України, який містить спеціальні норми, що визначають відповідальність за різні види кіберзлочинів. Зокрема, в розділі XVI йдеться про несанкціонований доступ до інформаційних систем, розроблення та розповсюдження шкідливого програмного забезпечення, а також втручання в роботу автоматизованих систем [8].

Одним із важливих нормативно-правових актів у сфері інформаційної безпеки є згадана вище Стратегія інформаційної безпеки, яка визначає актуальні загрози та виклики в інформаційній сфері, а також основні напрями державної політики для їх нейтралізації.

Основними положеннями Стратегії є ідентифікація внутрішніх і зовнішніх загроз, зокрема дезінформації, кібератак та інформаційних впливів, спрямованих на підрив державного суверенітету і територіальної цілісності України; посилення інституційної спроможності державних органів у сфері інформаційної безпеки, зокрема створення спеціалізованих центрів; захист критичної інформаційної інфраструктури від потенційних кібератак і несанкціонованого доступу; підвищення рівня медіаграмотності населення шляхом освітніх програм та інформаційних

кампаній; міжнародна співпраця для обміну досвідом і координації зусиль у протидії глобальним інформаційним загрозам.

Загалом Стратегія спрямована на формування стійкої та захищеної інформаційної екосистеми України, здатної ефективно протистояти сучасним викликам і загрозам в інформаційній сфері.

Після повномасштабного вторгнення російської федерації інформаційна безпека України стала відігравати ключову роль у забезпеченні національної стійкості та протидії ворожим впливам. Інформаційний простір стає не менш важливим полем бою, оскільки ворог активно застосовує інформаційні, кібернетичні та психологічні засоби для дестабілізації ситуації в країні. Основними загрозами в цей період є масові дезінформаційні кампанії, кібератаки на критичну інфраструктуру, інформаційно-психологічні операції (ІПСО), а також маніпуляції громадською думкою через соціальні мережі та засоби масової інформації.

Одним із найважливіших завдань держави є протидія дезінформації та ворожій пропаганді. В умовах війни противник активно використовує маніпулятивні технології для створення паніки серед населення, підриву довіри до державних інституцій та дестабілізації українського суспільства. Тому органи державної влади здійснюють оперативне виявлення та нейтралізацію фейкових новин, спростовують ворожі інформаційні атаки, а також ведуть системну комунікацію з громадянами через офіційні канали.

Валюшко І. О., досліджуючи трансформацію законодавства України у сфері інформаційної безпеки після російського вторгнення, зазначає, що агресія російської федерації на Сході України виявила непідготовленість українського суспільства одразу ж здійснити дієвий спротив агресору, спрямований на відновлення територіальної цілісності держави. Інформаційна сфера виявилася однією з найнезахищеніших в безпековому секторі України, виявивши серйозні прогалини у системі законодавчого забезпечення інформаційного простору. Проте разом з тим російське збройне втручання в Україну стало двигуном у напрацюванні відповідного законодавства в інформаційній сфері [9, с. 31].

Важливим чинником ефективної боротьби в інформаційному просторі є міжнародна співпраця у сфері інформаційної без-

пеки. Україна активно взаємодіє з міжнародними партнерами для протидії кібератакам, боротьби з пропагандою та дезінформацією. Співпраця з Європейським Союзом, НАТО та іншими міжнародними організаціями дозволяє отримувати підтримку у вигляді сучасних технологій, методологій інформаційної безпеки та доступу до передових розвідувальних даних.

Згідно зі звітом Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Державній службі спеціального зв'язку та захисту інформації України, у 2024 році було опрацьовано 4 315 кіберінцидентів. Це на 69,8 % більше, ніж у 2023 році, коли кіберзлочинці атакували український кіберпростір 2 541 раз. Найбільш поширеними цілями атак зловмисників є місцеві органи влади, урядові установи та організації, сектор безпеки та оборони, енергетичний сектор, комерційні компанії, телекомунікації.

Спеціалісти CERT-UA підкреслюють, що наразі спостерігається стійка тенденція до зростання кібератак, особливо на критично важливу інфраструктуру України. Ворог не полишає спроб дестабілізувати нашу країну і за допомогою кіберзброї. Це свідчить про те, що кіберпростір залишається одним із ключових напрямів воєнного протистояння [10].

Висновки. Таким чином, інформаційна безпека є невід'ємною складовою національної безпеки України, особливо в умовах сучасних викликів, пов'язаних із цифровізацією, інформаційною війною та гібридними загрозами. Аналіз поняття і змісту інформаційної безпеки свідчить про її багатогранність, що охоплює захист інформаційного простору, критичної інформаційної інфраструктури та інформаційного суверенітету держави. У законодавчому полі існує необхідність удосконалення нормативно-правового регулювання для забезпечення ефективного реагування на загрози, зокрема дезінформацію, кібератаки та маніпуляції суспільною свідомістю.

Державна політика в цій сфері має бути спрямована на забезпечення надійного захисту інформаційних ресурсів, формування інформаційної стійкості суспільства та ефективне протистояння зовнішнім і внутрішнім загрозам. Отже, вдосконалення механізмів інформаційної безпеки є ключовим фактором для збереження суверенітету, стабільності та сталого розвитку України.

Список використаних джерел

1. Стратегія інформаційної безпеки : затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 23.03.2025).

2. Проект Концепції інформаційної безпеки України / Organization for Security and Cooperation in Europe. URL: https://www.osce.org/uk/fom/175056 (дата звернення: 23.03.2025).

3. Гурковський В. І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства. *Правова інформатика*. 2010. № 2 (26). С. 72–77.

4. Баранов О. П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. *Вісник Національної академії державного управління при Президентові України.* 2014. № 3. С. 60–65.

5. Конституція України від 28.06.1996 № 254к/96-ВР. Дата оновлення: 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр/ed20200101#Text (дата звернення: 23.03.2025).

6. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 23.03.2025).

7. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 23.03.2025).

8. Кримінальний кодекс України від 05.04.2001 № 2341-III. Дата оновлення: 01.02.2025. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n2491 (дата звернення: 23.03.2025).

9. Валюшко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення. *Історико-політичні студії*. 2017. № 2 (8). С. 30–43.

10. CERT-UA минулого року опрацювала 4 315 кіберінцидентів / Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 23.03.2025).

Seletskyi O.,
PhD in Law, Associate Professor, Dean of the Faculty of Law,
Chernihiv Polytechnic National University, Chernihiv, Ukraine
ORCID: 0000-0002-8291-9736;
Kostiuchenko N.,
1st year master's student at the Faculty of Law,
Chernihiv Polytechnic National University, Chernihiv, Ukraine
ORCID: 0009-0005-3087-0191

THE CONCEPT AND CONTENT OF INFORMATION SECURITY AS A COMPONENT OF NATIONAL SECURITY

The article analyzes the concept and content of information security, based on regulatory legal acts and doctrinal approaches. It examines the main aspects that define information security in modern society and identifies the key elements that influence its formation and development. The role of information security in the structure of national security is determined. The importance of ensuring information security in the context of the full-scale invasion of the Russian Federation is emphasized. In the Information Security Strategy, information security in Ukraine is interpreted as an integral part of Ukraine's national security, referring to the state of protection of the state's sovereignty, territorial integrity, democratic constitutional order, and other vital interests of individuals, society, and the state. It ensures the proper protection of constitutional rights and freedoms of individuals regarding the collection, storage, use, and dissemination of information, access to reliable and objective information, and the existence of an effective system for protecting against and countering harm caused by the spread of negative informational influences. This includes coordinated dissemination of false information, destructive propaganda, other information operations, and unauthorized distribution, use, and violation of the integrity of restricted-access information. State policy in the field of information security should be aimed at ensuring reliable protection of information resources, forming the informational resilience of society, and effectively countering external and internal threats. Therefore, improving the mechanisms of information security is a key factor for preserving the sovereignty, stability, and sustainable development of Ukraine.

Key words: *information security, national security, cybersecurity, information protection, informational threats.*

References

1. President of Ukraine (2021), *Strategy of Information Security*, Decree No. 685/2021, 28 December, available at: https://zakon.rada.gov.ua/laws/show/685/2021#Text (accessed 23 March 2025).

2. Organization for Security and Cooperation in Europe (n.d.), *Draft Concept of Information Security of Ukraine,* available at: https://www.osce.org/uk/fom/175056 (accessed 23 March 2025).

3. Hurkovskyi, V. I. (2010), "Security as an Object of Legal Relations in the Conditions of the Global Information Society", *Legal Informatics*, № 2 (26), pp. 72–77.

4. Baranov, O. P. (2014), "Preconditions for the Creation of the State Special Transport Service and Its Tasks in the System of National Security of Ukraine", *Bulletin of the National Academy of Public Administration under the President of Ukraine*, № 3, pp. 60–65.

5. Verkhovna Rada of Ukraine (1996), *Constitution of Ukraine*, Law No. 254к/96-VR, 28 June, available at: https://zakon.rada.gov.ua/laws /show/254к/96-вр/ed20200101#Text (accessed 23 March 2025).

6. Verkhovna Rada of Ukraine (2018), *On National Security of Ukraine*, Law No. 2469-VIII, 21 June, available at: https://zakon.rada.gov. ua/laws/show/2469-19#Text (accessed 23 March 2025).

7. Verkhovna Rada of Ukraine (1992), *On Information*, Law No. 2657-XII, 2 October, available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text (accessed 23 March 2025).

8. Verkhovna Rada of Ukraine (2001), *Criminal Code of Ukraine*, Law No. 2341-III, 5 April, available at: https://zakon.rada.gov.ua/laws/ show/2341-14#n2491 (accessed 23 March 2025).

9. Valyushko, I. O. (2017), "Information Security of Ukraine: Transformation of Legislation After the Russian Invasion", *Historical and Political Studies*, № 2(8), pp. 30–43.

10. State Service of Special Communications and Information Protection of Ukraine (2024), 'CERT-UA Processed 4315 Cyber Incidents Last Year', available at: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (accessed 23 March 2025).