

УДК 342.9

DOI <https://doi.org/10.24144/2788-6018.2025.01.94>

ДО ПИТАННЯ КОНСТИТУЦІЙНИХ ЗАСАД ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Шевчук М.О.,

*кандидат юридичних наук,
докторант кафедри конституційного, адміністративного
та фінансового права,
Хмельницький університет управління та права
імені Леоніда Юзькова
ORCID: 0000-0001-7549-6344*

Шевчук М.О. До питання конституційних засад інформаційної безпеки держави.

Метою цієї статті є дослідження конституційних засад інформаційної безпеки держави, зокрема принципів політичного та ідеологічного плюралізму, пріоритету прав та свобод людини, верховенства права, своєчасності та доцільності заходів протидії загрозам інформаційної безпеки, а також державного й громадського контролю у цій сфері. Інформаційна безпека є невід'ємною складовою національної безпеки держави, і її забезпечення потребує комплексного підходу, що поєднує правові, соціальні та технічні заходи. Конституційні положення відіграють ключову роль у створенні правової основи для захисту інформаційного простору, проте їх реалізація повинна враховувати сучасні виклики та загрози.

Забезпечення інформаційної безпеки повинно базуватися на балансі між правами громадян на доступ до інформації, свободою слова та необхідністю захисту держави. Цей баланс є важливим для уникнення зловживань з боку держави та забезпечення демократичних стандартів.

Сучасні виклики, такі як дезінформація, кібератаки та маніпуляції громадською думкою, потребують адаптації національного законодавства до міжнародних стандартів. Зокрема, важливо впроваджувати рекомендації ЄС, ООН та інших міжнародних організацій у національну правову систему.

Методологія дослідження базується на аналізі нормативно-правових актів, наукових джерел, а також порівняльному аналізі відповідних положень міжнародного права. Наукова новизна полягає у комплексному підході до визначення конституційних основ інформаційної безпеки, що є актуальним у контексті сучасних загроз інформаційного простору. Висновки підкреслюють важливість вдосконалення законодавчої бази України в сфері інформаційної безпеки, а також необхідність підвищення ефективності контролю за дотриманням інформаційних прав і свобод як з боку держави, так і з боку громадськості. Роль органів державної влади у забезпеченні інформаційної безпеки є критичною. Необхідно посилювати координацію між різними відомствами, створювати спеціалізовані органи, відповідальні за моніторинг інформаційного простору, та забезпечувати прозорість їх діяльності.

Ключові слова: конституційні засади, права людини, політичний плюралізм, державний контроль, інформаційні загрози.

Shevchuk M.O. On the issue of constitutional principles of state information security.

The purpose of this article is to study the constitutional foundations of the State's information security, in particular, the principles of political and ideological pluralism, the priority of human rights and freedoms, the rule of law, timeliness and appropriateness of measures to counter information security threats, and state and public control in this area. Information security is an integral part of the national security of the state, and its provision requires a comprehensive approach that combines legal, social and technical measures. Constitutional provisions play a key role in creating a legal framework for the protection of the information space, but their implementation should take into account current challenges and threats.

Information security should be based on a balance between the rights of citizens to access information, freedom of speech and the need to protect the state. This balance is important to avoid abuse by the state and to ensure democratic standards.

Modern challenges, such as disinformation, cyberattacks and manipulation of public opinion, require the adaptation of national legislation to international standards. In particular, it is important to implement the recommendations of the EU, the UN and other international organisations into the national legal system.

The research methodology is based on the analysis of legal acts, scientific sources, and a comparative analysis of the relevant provisions of international law. The scientific novelty lies in the comprehensive approach to defining the constitutional foundations of information security, which is relevant in the context of modern threats to the information space. The conclusions emphasise the importance of improving the legislative framework of Ukraine in the field of information security, as well as the need to increase the effectiveness of control over the observance of information rights and freedoms by both the State and the public. The role of public authorities in ensuring information security is critical. It is necessary to strengthen coordination between different agencies, to create specialised bodies responsible for monitoring the information space, and to ensure transparency of their activities.

Key words: constitutional principles, human rights, political pluralism, state control, information threats.

Постановка проблеми. Інформаційна безпека держави є однією з ключових складових національної безпеки, особливо в умовах сучасного інформаційного простору, що є ареною для різноманітних загроз, пов'язаних із дезінформацією, кіберзлочинністю та інформаційними війнами. З огляду на це, важливим є забезпечення відповідних конституційних гарантій та правових механізмів, які б забезпечували захист інформаційного простору держави і її громадян [1].

Аналіз останніх досліджень і публікацій. Питання конституційних засад інформаційної безпеки розглядалися в працях таких науковців, як О.І. Зозуля, який акцентував увагу на значенні конституційних принципів для забезпечення інформаційної безпеки України [1], а також Т.В. Чубарук, яка досліджувала правове регулювання інформаційної сфери [5]. Дослідження В.В. Шемчука присвячені порівняльно-правовому аналізу забезпечення інформаційної безпеки в різних державах [6]. Водночас, окремі аспекти цього питання, зокрема державний і громадський контроль у сфері інформаційної безпеки, залишаються недостатньо дослідженими.

Незважаючи на значну кількість наукових праць, що присвячені інформаційній безпеці, питання конституційних засад цієї сфери потребує подальшого дослідження, особливо з огляду на нові виклики, що виникають у сучасному інформаційному середовищі. Зокрема, потребує детальнішого аналізу роль політичного й ідеологічного плюралізму, а також пріоритету прав людини в контексті інформаційної безпеки.

Мета статті – дослідження конституційних засад інформаційної безпеки держави, зокрема таких принципів, як політичний та ідеологічний плюралізм, пріоритет прав та свобод людини, верховенство права, своєчасність та доцільність заходів протидії загрозам інформаційної безпеки, а також державний і громадський контроль у цій сфері.

Виклад основного матеріалу. У контексті України конституційні засади інформаційної безпеки є ключовим елементом правового регулювання. Вони визначають напрями захисту інформаційного простору та впливають на формування національної політики у цій сфері.

Основними принципами, що лежать в основі конституційної моделі інформаційної безпеки, можемо визначити: політичний та ідеологічний плюралізм; пріоритет прав і свобод людини; верховенство права; своєчасність і доцільність заходів протидії загрозам; державний і громадський контроль.

Ці принципи знайшли своє відображення в Конституції України, яка встановлює основи правового регулювання інформаційного простору та забезпечення національної безпеки.

Таким чином, конституційні основи інформаційної безпеки визначаються рядом принципів, що закріплені в національному законодавстві та міжнародних правових актах. До них належать принцип політичного й ідеологічного плюралізму, пріоритет прав та свобод людини, принцип верховенства права, своєчасність та доцільність заходів протидії загрозам інформаційної безпеки, а також державний та громадський контроль у цій сфері.

Політичний та ідеологічний плюралізм є одним із основоположних принципів демократичної держави, який сприяє забезпеченню інформаційної безпеки. У контексті конституційних засад інформаційної безпеки, цей принцип передбачає можливість різних політичних та ідеологічних поглядів співіснувати в межах одного інформаційного простору, що дозволяє уникнути монополії на інформацію та забезпечує можливість вільного доступу до різних джерел інформації [2].

Законодавчі акти України підкреслюють важливість політичного та ідеологічного плюралізму як засобу захисту від інформаційних загроз, зокрема у контексті пропагандистських атак та дезінформації. У цьому зв'язку варто зазначити, що інформаційна безпека має будуватися на засадах плюралізму, що дозволяє уникнути інформаційного диктату та забезпечує свободу слова [3].

Пріоритет прав і свобод людини є невід'ємною складовою конституційних засад інформаційної безпеки. Конституція України гарантує права:

1. на свободу думки і слова, вільне вираження своїх поглядів і переконань,

2. право на інформацію,
3. право на захист особистого життя та конфіденційної інформації [6].

Ці права тісно пов'язані із забезпеченням інформаційної безпеки, оскільки держава повинна захищати громадян не тільки від зовнішніх загроз, але й забезпечувати захист їхніх прав в інформаційному просторі.

Забезпечення інформаційної безпеки повинно відбуватися з дотриманням основоположних прав і свобод людини, закріплених у Конституції України. Пріоритет прав людини в інформаційній сфері означає, що будь-які заходи, спрямовані на забезпечення безпеки інформаційного простору, не можуть порушувати права на інформацію, свободу слова та право на приватність [4].

Законодавство України визначає право на доступ до інформації як одне з ключових прав людини, яке повинно бути захищене навіть у контексті забезпечення національної безпеки [11]. Це вимагає від держави забезпечення балансу між захистом інформаційного простору та дотриманням прав громадян на вільний доступ до інформації.

Принцип верховенства права є ключовою конституційною засадою, яка визначає всі аспекти функціонування держави, включно із сферою інформаційної безпеки.

Цей принцип передбачає, що всі суб'єкти правовідносин – і держава, і громадяни – діють у межах закону. У сфері інформаційної безпеки це означає, що заходи, спрямовані на протидію загрозам, мають ґрунтуватися на правових нормах, бути обґрунтованими та пропорційними [5].

Згідно з цим принципом, держава зобов'язана забезпечувати чіткі та прозорі правові механізми для захисту інформаційного простору. Це включає як розробку законів, що регулюють діяльність в інформаційній сфері, так і забезпечення їх ефективного виконання. Принцип верховенства права також вимагає, щоб будь-які обмеження прав і свобод громадян в інформаційній сфері мали законодавче підґрунтя та не порушували основоположних прав людини [7].

Застосування принципу верховенства права у сфері інформаційної безпеки також передбачає наявність ефективних механізмів судового контролю за діяльністю органів, що забезпечують інформаційну безпеку. Громадяни повинні мати можливість оскаржувати рішення та дії державних органів у випадку, якщо вони вважають, що їхні права було порушено внаслідок заходів, спрямованих на забезпечення інформаційної безпеки [12].

Принцип верховенства права передбачає, що всі суб'єкти правовідносин, включаючи органи державної влади, повинні діяти в межах закону. У сфері інформаційної безпеки це означає, що держава повинна здійснювати свою діяльність на основі правових норм, забезпечуючи прозорість і підзвітність своїх дій.

У сфері інформаційної безпеки принцип верховенства права означає, що держава повинна здійснювати свою діяльність в інформаційній сфері виключно на законних підставах, дотримуючись прав і свобод громадян та забезпечуючи прозорість і підзвітність своїх дій. Це включає в себе створення чіткої правової бази для регулювання інформаційної безпеки, яка повинна відповідати як міжнародним стандартам, так і національним інтересам.

Слід зазначити, що згідно з принципом верховенства права, будь-які заходи, спрямовані на забезпечення інформаційної безпеки, повинні бути пропорційними, обґрунтованими та співмірними з тими загрозами, проти яких вони спрямовані.

Важливим аспектом є також судовий контроль за діями органів державної влади у сфері інформаційної безпеки, що гарантує захист прав громадян від можливих зловживань з боку держави [5].

Верховенство права забезпечує також правову визначеність та стабільність у сфері інформаційної безпеки, що є необхідним для ефективної протидії новим викликам і загрозам у сучасному інформаційному середовищі. Наприклад, у законодавстві України про національну безпеку та інформаційну безпеку передбачено, що всі заходи мають відповідати Конституції та іншим правовим нормам, а у випадку порушення цих норм громадяни мають право на звернення до суду для захисту своїх прав [6].

Заходи у сфері інформаційної безпеки мають бути пропорційними загрозам, проти яких вони спрямовані, і не повинні порушувати прав громадян. Судовий контроль за діями органів державної влади у цій сфері забезпечує захист від зловживань і сприяє дотриманню принципу законності [5].

Одним із ключових елементів забезпечення інформаційної безпеки є своєчасність та доцільність заходів, що вживаються для протидії загрозам у цій сфері. Загрози інформаційній безпеці можуть мати різний характер – від кібератак до інформаційних операцій, спрямованих на дестабілізацію суспільства. Тому державні органи повинні мати можливість оперативно реагувати на такі загрози, водночас дотримуючись правових норм і принципів [9].

Своєчасність заходів полягає у швидкому виявленні загроз та їх нейтралізації, що є особливо важливим в умовах сучасних інформаційних війн. Доцільність заходів передбачає, що вони мають бути пропорційними до рівня загрози та не порушувати основних прав і свобод громадян. Напри-

клад, кібербезпекові заходи повинні бути спрямовані на захист критичної інфраструктури, державних інформаційних ресурсів та приватних даних громадян [8].

У цьому контексті важливе значення має Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення кібербезпеки держави, а також механізми взаємодії між державними органами, приватним сектором та громадськістю у цій сфері [13].

Цей принцип спрямований на оперативне реагування на загрози в інформаційному просторі. Конституція України передбачає, що держава повинна вживати всіх необхідних заходів для захисту інформаційного простору, дотримуючись при цьому прав і свобод громадян [7].

Слід звернути увагу на те, що у сучасних умовах важливу роль відіграє система раннього попередження та моніторингу інформаційних загроз, що дозволяє своєчасно виявляти дезінформацію, пропаганду або кібератаки й розробляти відповідні заходи реагування.

Державний та громадський контроль також є важливою складовою забезпечення інформаційної безпеки, оскільки вони дозволяють забезпечити прозорість та ефективність заходів, що вживаються у цій сфері. Державний контроль здійснюється через спеціалізовані органи, що відповідають за захист інформаційного простору, зокрема Службу безпеки України, Національну комісію з питань регулювання зв'язку та інформатизації, а також інші органи, що займаються забезпеченням кібербезпеки та захистом інформаційних ресурсів держави. Ці органи мають повноваження здійснювати моніторинг інформаційного простору, виявляти потенційні загрози та вживати відповідних заходів для їх нейтралізації [14].

Громадський контроль, у свою чергу, є важливим механізмом забезпечення прозорості та підзвітності державної політики у сфері інформаційної безпеки. Він полягає у залученні громадянського суспільства, незалежних експертів, засобів масової інформації та правозахисних організацій до процесу оцінки заходів, що вживаються державою для забезпечення інформаційної безпеки. Це дозволяє підвищити рівень довіри до таких заходів, а також забезпечити дотримання прав людини та демократичних стандартів [5].

Громадський контроль може здійснюватися через різні форми, включаючи публічні дебати, незалежні розслідування, моніторинг дотримання прав і свобод у ході реалізації державної політики у сфері інформаційної безпеки. Важливим аспектом є також роль громадських організацій у підготовці законодавчих ініціатив, що стосуються інформаційної безпеки, а також у контролі за їх реалізацією [10].

Отже, громадський контроль є невід'ємною складовою демократичного суспільства. Громадські організації та незалежні експерти беруть участь у моніторингу інформаційного простору, виявленні маніпуляцій та спростуванні дезінформації. Це сприяє підвищенню прозорості й відповідальності державних органів [10].

На сучасному етапі розвитку інформаційного суспільства конституційні засади інформаційної безпеки стикаються з новими викликами, що пов'язані з глобалізацією інформаційних процесів, розвитком комп'ютерних технологій та поширенням соціальних мереж. Одним із ключових викликів є необхідність адаптації національного законодавства до нових реалій інформаційної безпеки, зокрема у контексті захисту прав громадян в умовах кіберзагроз [7].

Також важливим питанням є забезпечення ефективної міжнародної співпраці у сфері інформаційної безпеки. Інформаційні загрози часто мають транснаціональний характер, тому їх нейтралізація вимагає координації зусиль на міжнародному рівні. Україна активно співпрацює з міжнародними організаціями, зокрема ООН та ОБСЄ, у сфері забезпечення інформаційної безпеки, що сприяє обміну досвідом та впровадженню новітніх технологій у боротьбі з інформаційними загрозами [4].

Перспективи розвитку конституційних засад інформаційної безпеки також пов'язані з удосконаленням механізмів забезпечення кібербезпеки, розвитку національної інформаційної інфраструктури та підвищенням рівня інформаційної грамотності населення. Ці заходи сприятимуть підвищенню стійкості держави до інформаційних загроз та забезпеченню стабільності інформаційного простору [6].

Конституційні засади інформаційної безпеки держави є важливим елементом забезпечення національної безпеки та захисту прав і свобод громадян. До них належать принципи політичного та ідеологічного плюралізму, пріоритет прав і свобод людини, принцип верховенства права, своєчасність та доцільність заходів протидії загрозам інформаційної безпеки, а також державний та громадський контроль у цій сфері. Забезпечення цих принципів є ключовим для ефективної протидії сучасним інформаційним загрозам та збереження демократичних цінностей у суспільстві.

Держава повинна постійно вдосконалювати правові механізми, що регулюють інформаційну безпеку, беручи до уваги нові виклики та загрози, що виникають в умовах розвитку інформаційних технологій. Важливою умовою забезпечення інформаційної безпеки є також залучення громадянського суспільства до процесу прийняття рішень та контролю за діяльністю державних органів у

цій сфері. Лише комплексний підхід, що враховує як правові, так і технологічні аспекти, дозволить забезпечити належний рівень інформаційної безпеки держави та захист прав і свобод громадян в інформаційному просторі.

Висновки. У результаті дослідження було встановлено, що основними конституційними засадами інформаційної безпеки є принципи політичного та ідеологічного плюралізму, пріоритет прав і свобод людини, верховенство права, своєчасність і доцільність заходів протидії загрозам інформаційної безпеки, а також державний і громадський контроль у цій сфері. Всі ці принципи є взаємопов'язаними і спрямовані на забезпечення стабільності інформаційного простору держави, а також на захист прав і свобод громадян.

Принцип політичного і ідеологічного плюралізму підкреслює важливість забезпечення різноманітності думок і поглядів у суспільстві, що сприяє демократизації інформаційного простору та запобігає монополізації інформації, що особливо важливо в умовах сучасних інформаційних загроз, таких як дезінформація та пропаганда, які можуть використовуватися для маніпуляції громадською думкою і дестабілізації суспільства.

Пріоритет прав і свобод людини є ключовим у процесі забезпечення інформаційної безпеки, оскільки він стоїть на захисті права громадян на інформацію, свободу слова та приватність. Це означає, що заходи держави з протидії загрозам інформаційної безпеки не повинні порушувати ці права, а всі дії повинні бути збалансованими та відповідати конституційним нормам.

Принцип верховенства права гарантує, що всі заходи щодо забезпечення інформаційної безпеки будуть здійснюватися в рамках закону і контролюватися судовою владою. Це забезпечує юридичну прозорість і запобігає можливим зловживанням з боку держави. Важливим є також забезпечення своєчасності та доцільності заходів, які вживаються для захисту інформаційного простору, оскільки це дозволяє державі оперативно реагувати на нові виклики та загрози.

Державний і громадський контроль є не менш важливими елементами системи інформаційної безпеки. Вони забезпечують прозорість діяльності державних органів, підвищують ефективність заходів щодо протидії загрозам і сприяють залученню громадянського суспільства до процесу забезпечення безпеки.

Подальші дослідження в сфері конституційних засад інформаційної безпеки повинні бути спрямовані на розробку механізмів ефективної взаємодії між державою та громадськістю в контексті забезпечення інформаційної безпеки. Крім того, важливим є дослідження нових викликів, таких як кіберзлочинність і інформаційні війни, які потребують нових підходів до правового регулювання інформаційного простору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Зозуля О.І. Конституційні засади інформаційної безпеки України. *Форум права*. 2020. № 4. С. 32–44. URL: http://forumprava.pp.ua/files/032-044-2020-4-FP-Zozulia_6.pdf.
2. Про засади інформаційної безпеки України: Проект Закону України від 28.05.2014 № 4949. URL: <https://ips.ligazakon.net/document/JG3TH00A>.
3. Конституційно-правові засади інформаційної безпеки у парадигмі «війни нового покоління». URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/93d3b777-67b5-41c5-a926-382051e2d786/content>.
4. Концепція інформаційної безпеки України: проект. URL: <https://www.osce.org/files/f/documents/0/2/175056.pdf>.
5. Чубарук Т.В. Конституційні засади правового регулювання інформаційної сфери. *Правова інформатика*, 2010 р. URL: <https://ippi.org.ua/sites/default/files/10ctvris.pdf>.
6. Шемчук В.В. Конституційно-правове забезпечення інформаційної безпеки сучасних держав: порівняльно-правовий аналіз. Ужгород, 2020 р. URL: <https://www.uzhnu.edu.ua/uk/infocentre/get/30788>.
7. Шемчук В.В. Конституційно-правові засади розвитку інформаційного суспільства в Україні. *Науковий вісник Національної академії внутрішніх справ*. № 3 (108), 2018 р. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/6791/1/Nvknivs_2018_3_13.pdf.
8. Шевчук М.О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. Випуск 78: частина 2. С. 134–139. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/08/23.pdf>.
9. Єсімов С.С. Конституційні основи адміністративно-правового режиму інформаційної безпеки. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2018. Випуск 4. С. 134–142. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/2618/1/20118-4-16.pdf>.

10. Котерлін І.Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 1. С. 150–156. URL: http://apnl.dnu.in.ua/1_2022/25.pdf.
11. Міжнародний пакт про громадянські і політичні права (ратифіковано Указом Президії Верховної Ради Української РСР № 2148-viii від 19.10.1973. URL: https://zakon.rada.gov.ua/laws/show/995_043.
12. Коментарі до проекту Закону України «Про інформаційну безпеку України» (від 22.09.2004 р. № 5732). Харківська правозахисна група. URL: <http://khpg.org/index.php?id=1105737155>.
13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Офіційний вісник України*. 2017. № 91. Ст. 2765. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>.
14. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. *Офіційний вісник України*. 2018. № 55. Ст. 1903. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>.