НАУКОВІ ТА НАВЧАЛЬНО-МЕТОДИЧНІ ПУБЛІКАЦІЇ ПРОФЕСОРСЬКО-ВИКЛАДАЦЬКОГО СКЛАДУ

С. Байрак – кандидат політичних наук, доцент кафедри політології та публічного управління ВНУ імені Лесі Українки

Концептуальні засади дослідження державної політики у сфері забезпечення інформаційної безпеки

Під час формування сучасного суспільства, інформація набула критичного значення для розвитку цивілізації. Вона впливає на всі сфери людського життя та перетворює уявлення про роль інформаційних ресурсів. Умови глобалізації сприяють інтеграції національних інформаційних систем у єдину міжнародну мережу, що призводить до утворення спільного інформаційного простору та розширення міжнародних інформаційно-телекомунікаційних зв'язків. Забезпечення безпеки в інформаційному просторі є пріоритетом для будь-якої сучасної держави і ключовою умовою для її стійкого розвитку. Недосконаліть заходів безпеки може призвести до значних системних відмов у соціально-політичних, економічних, технологічних та інших сферах суспільства, що може знизити ефективність органів державної влади та вплинути на їх здатність виконувати свої функції.

У контексті України, особливо важливим є питання підвищення ефективності роботи органів публічної влади у сфері безпеки в інформаційному просторі, особливо в умовах російсько-української війни. Це охоплює не лише розробку стратегій та політик, але й їх успішну реалізацію з метою захисту інформаційного простору держави від потенційних загроз.

У сучасному політичному процесі роль інформаційної політики держави набуває великого значення, що зумовлено переходом розвинутих країн до епохи інформаційного суспільства. Упродовж цього

часу засоби масової інформації пройшли шлях від простих засобів відображення реальності до потужних інструментів, які активно формують цю реальність.

Г. Почепцов вважає, що інформаційну політику слід тлумачити як сукупність принципів та підходів, що визначають закони функціонування інформаційної сфери. Це охоплює розуміння того, як інформація поширюється, обробляється, зберігається та використовується в суспільстві, а також як вона впливає на громадську думку, політичні рішення та соціальні процеси [1, с. 12].

Важливо зазначити, що сучасна інформаційна політика включає не лише керування засобами масової інформації, але й адаптацію до нових цифрових технологій та інтернет-комунікацій, що дозволяє державам використовувати інформацію як засіб впливу та контролю.

Концепція інформаційної безпеки на сьогоднішній день ще не досягла повної зрілості, що підкреслює потребу в більш систематизованому підході. Дослідник у сфері державного управління З. Коваль, визначає інформаційну безпеку держави як захист інформації та цілісності критично важливої інформаційної інфраструктури від випадкових чи умисних впливів, що можуть мати природній або штучний характер [2, с. 11].

В. Фомін і А. Рось розглядають поняття інформаційної безпеки в межах національної безпеки кожної держави як бажання країн здійснити та захистити свої національні інтереси. Особливу важливість у цьому процесі вони приділяють формуванню та накопиченню національного інформаційного потенціалу, що стає актуальним у зв’язку з глобалізацією світових інформаційних процесів [3, с. 24].

Ці підходи відображають важливість інформації як стратегічного ресурсу в сучасному світі. У зв’язку з глобалізацією та поширенням цифрових технологій, здатність ефективно зберігати, контролювати та використовувати інформацію стає ключовою для національної безпеки держави та захисту її національних інтересів. Це означає не лише захист від зовнішніх інформаційних загроз, а й розвиток внутрішніх інформаційних ресурсів і технологій, які можуть бути використані для підтримки національного розвитку та забезпечення благополуччя.

Український вчений В. Тертичка визначає термін «державна політика» як «відносно стабільна, організована й цілеспрямована діяльність/

бездіяльність державних інституцій, здійснювана ними безпосередньо чи опосередковано щодо певної проблеми або сукупності проблем, яка впливає на життя суспільства» [4, с. 82–83]. О. Дем'янчук зі свого боку розглядає поняття «державна політика», як «наміри уряду вжити певних заходів загального характеру задля розв'язання певних значних державних завдань, тобто, для реалізації державної влади» [5, с. 32].

Це дає змогу стверджувати, що основна мета державної політики в сфері інформаційної безпеки полягає в керуванні реальними та потенційними загрозами для створення умов, що задовольняють інформаційні потреби людини та громадянина, сприяють реалізації національних інтересів тощо.

За висловами Р. Шаповала та В. Клочка, державна політика України у сфері інформаційної безпеки полягає в діяльності державно-правових інституцій, спрямованій на управління загрозами та небезпеками. Це необхідно для задоволення інформаційних потреб і реалізації національних інтересів [6, с. 6].

Отже, інформаційна безпека виступає як невід'ємна складова загальної державної інформаційної політики. Вона охоплює комплекс заходів економічного, політичного та організаційного характеру, які є адекватними для протидії загрозам національній безпеці та забезпечують управління ризиками. Система забезпечення інформаційної безпеки діє як інструмент реалізації відповідної державної політики і спрямована на досягнення цілей національної безпеки в інформаційній сфері. Важливим аспектом такої системи є створення збалансованого простору співіснування інтересів особи, суспільства та держави в інформаційному просторі.

З врахуванням наведеного аналізу можна казати, що державна політика у сфері інформаційної безпеки орієнтується на три ключові напрями:

Захист інформаційних прав і свобод людини – включає захист персональних даних, свободи слова та доступу до інформації. Мета полягає в гарантуванні прав і свобод громадян у сфері інформації, запобіганні цензурі та обмеженню свободи вираження поглядів.

Захист державної безпеки в інформаційній сфері – охоплює діяльність, спрямовану на протидію інформаційним загрозам національній безпеці, таким як кібератаки, інформаційні війни та шпигунство.

Основна мета – захист критично важливої інформаційної інфраструктури та запобігання втручанню у внутрішні справи держави.

Захист національного інформаційного ринку та економічних інтересів держави в інформаційній сфері – включає заходи для підтримки та розвитку національних виробників інформаційної продукції, а також захист від недобросовісної конкуренції та монополізації інформаційного простору. Основна мета – підтримка здорового, конкурентоспроможного та різноманітного інформаційного ринку [7, с. 146].

Інформаційна безпека представляє собою складне, багаторівневе і системне явище, що залежить від багатьох чинників, включаючи зовнішні та внутрішні. Серед її найважливіших чинників можна виділити такі:

1) глобальну політичну ситуацію;

2) потенційні зовнішні та внутрішні загрози;

3) рівень розвитку інформаційно-комунікаційних технологій у країні;

4) політичну обстановку в межах держави.

Інформаційна безпека також розглядається як динамічна, цілісна соціальна система, що включає безпеку особистості, держави та суспільства. Важливо розуміти, що ці підсистеми є взаємопов’язаними і формують систему, що гарантує захист життєво важливих інтересів людини, суспільства і держави, сприяючи їх конкурентоспроможному і прогресивному розвитку [8, с. 154–155].

За словами М. Криштановича, в галузі публічного управління, політика держави в сфері інформаційної безпеки охоплює широкий спектр заходів. Ці заходи включають захист національного інформаційного простору, інтеграцію країни в світовий інформаційний простір, а також виявлення та усунення причин дискримінації у сфері інформації. Політика також передбачає необхідність запобігання порушенням у національному інформаційному просторі та протидію інформаційній експансії інших країн. Крім того, вона передбачає розроблення та впровадження спеціальних засобів та методів для підвищення ефективності зберігання, використання та поширення інформаційних даних національного значення, а також формування ефективної інформаційної інфраструктури та її стабільного розвитку [9, с. 251].

Згідно з думкою М. Гаврильціва, політика держави у сфері безпеки інформаційного простору розглядається як система державних заходів, спрямованих на вирішення ключових завдань у різних галузях, таких

як економіка, військово-політична сфера, соціальний сектор та інші [10, с. 201].

Політика в цій сфері може бути охарактеризована як складне явище, що охоплює аспекти економічного, зовнішньополітичного, військового та технологічного характеру. Важливо, щоб діяльність органів публічної влади спрямовувалася на створення умов для ефективної реалізації цих заходів з метою забезпечення високого рівня безпеки в інформаційному середовищі [11]. За словами Є. Архипова та А. Черниченка, ця політика представляє собою процес, що включає розвиток організаційно-технічних компонентів та нормативної бази в цій сфері. Забезпечення безпеки в інформаційному середовищі держави є ключовим аспектом діяльності органів публічної влади, який базується на нормах чинного законодавства та міжнародного права. Таким чином, ця політика не лише визначається як статичне явище, але й передбачає постійну адаптацію до змінюваних умов та викликів інформаційного середовища [12, с. 233].

Згідно з дослідженнями, зокрема роботами Я. Малика, політика держави у сфері забезпечення інформаційної безпеки розглядається як діяльність, що ґрунтується на пріоритетності загальнонаціональних інтересів. Це включає розуміння потенційних інформаційних загроз та небезпек, а також впровадження відповідних державних програм, концепцій та стратегій у цій сфері з урахуванням положень чинного законодавства [13, с. 14].

Отже, цей напрям діяльності держави потребує комплексного підходу, що включає стратегічне планування, реагування на загрози, а також законодавчу та організаційну підтримку. Гарантування безпеки інформаційного простору не лише важливе для захисту державних і суспільних інтересів, але й для підтримки стабільності та розвитку в світі, де інформація є одним з ключових ресурсів.

Успішна реалізація політики держави у сфері безпеки інформаційного простору значною мірою залежить від ефективності управлінських рішень, які приймаються представниками органів публічної влади. Це включає ухвалення нормативно-правових актів, які регулюють інформаційні відносини та встановлюють механізми контролю за їх дотриманням.

Згідно з науковими дослідженнями О. Кириченка, для ефективного забезпечення безпеки в інформаційному просторі важливо створити та впровадити уніфіковану систему економічної безпеки національного

значення. Ця система повинна ґрунтуватися на принципах комплексності, системності, спрямованості, єдності, безперервності та інших. Крім того, важливою є здатність цієї системи постійно адаптуватися до змін у внутрішньому та зовнішньому середовищі, реагувати на нові загрози та виклики і, відповідно, створювати умови, що відповідають вимогам сучасного світу та процесам розвитку інформаційного суспільства [14, с. 22].

Так, постійний моніторинг та оновлення політики та стратегій у сфері інформаційної безпеки є критичними в умовах швидкозмінюваного цифрового світу. При визначенні понятійно-категоріального апарату забезпечення інформаційної безпеки важливо враховувати різні механізми публічного адміністрування, що використовуються у цій сфері. Одним із таких механізмів є державно-правовий, який, згідно з поглядами О. Федорчука, можна розглядати як комплекс дій, спрямованих на створення умов для ефективної реалізації державної інформаційної політики.

Цей підхід підкреслює важливість інтегрованого та системного підходу до сфери інформаційної безпеки. Він включає розробку та впровадження відповідних законодавчих та нормативних актів, координацію між різними органами влади, а також розробку і застосування конкретних стратегій і процедур. Такий підхід сприяє створенню комплексної системи заходів, яка максимально ефективно захищає інформаційний простір від потенційних загроз [15, с. 184].

Державно-правовий механізм публічного адміністрування у сфері безпеки інформаційного простору можна розглядати як цілісну систему, що складається з органів публічної влади та спеціалізованих установ. Ці елементи формують нормативно-правове поле відповідної сфери та забезпечують ефективне регулювання економічних, фінансових, господарських та суспільних відносин між різними суб’єктами, задіяними у забезпеченні безпеки інформаційного простору та захисті інформаційних даних.

Згідно з А. Сліпчуком, організаційно-правовий механізм представляє собою систему державних органів, що відповідають за ефективне впровадження політики інформаційної безпеки. Важливим аспектом є система законодавчих норм, яка регулює взаємодії між учасниками в цій сфері. Також, до складових механізму входить сукупність органів влади та цивільних інститутів, які відповідають за формування та реалізацію державної політики забезпечення інформаційної безпеки.

Такі механізми підкреслюють важність координації та об'єднання зусиль різних органів влади, а також залучення громадянського суспільства до процесу формування та втілення державної політики в сфері інформаційної безпеки. Це допомагає краще реагувати на сучасні виклики та загрози в інформаційному середовищі і більш повно розглядати різноманітні аспекти інформаційної безпеки.

Іншим важливим елементом державної політики у сфері інформаційної безпеки є правові відносини, що виникають між різними учасниками у процесі реалізації національної стратегії у цій області. Ці відносини включають комплекс методів та алгоритмів дій, які представники державних органів використовують для підвищення ефективності державної політики.

Правовий аспект цього механізму включає ієрархічну систему законодавчих принципів та норм, які регулюють діяльність державних та громадських інституцій з метою забезпечення безпеки в інформаційному просторі. Це означає, що ефективне управління в цій сфері потребує не лише розуміння та використання відповідних законів та норм, але й розробки та впровадження спеціалізованих методів і підходів [11].

Така правова основа сприяє створенню систематизованого та прозорого середовища, де можна ефективно вирішувати питання, пов'язані з інформаційною безпекою, з урахуванням національних та міжнародних вимог і стандартів. Це сприяє розвитку стабільного та безпечного інформаційного простору, що має велике значення для захисту інтересів держави та громадянського суспільства.

Організаційно-правовий механізм публічного адміністрування у сфері забезпечення інформаційної безпеки держави відіграє ключову роль у формуванні та реалізації державної політики. Цей механізм включає розробку системи організаційно-управлінських заходів, спрямованих на втілення ключових аспектів стратегії національної безпеки. Одним з головних завдань є вдосконалення законодавчої бази в цій сфері, створення системи оцінювання рівня інформаційної безпеки та розробка ефективних механізмів саморегуляції в цій галузі.

Цей механізм представляє собою систему органів публічної влади, що відповідають за розробку та впровадження державної політики у сфері інформаційної безпеки. Це підкреслює значення координації діяльності різних органів влади у цьому напрямі.

Визначення організаційно-правового механізму забезпечення інформаційної безпеки держави дозволяє гармонізувати розробку нормативно-правової бази відповідно до сучасних досягнень у сфері інформаційних технологій. Крім того, цей механізм включає в себе створення послідовності дій для органів влади з метою ефективної реалізації державної політики у сфері інформаційної безпеки, враховуючи наявні ресурси та забезпечуючи контроль за їх використанням. Це сприяє створенню гнучкої, адаптивної системи, яка може ефективно реагувати на швидкі зміни у галузі інформаційних технологій та цифрової безпеки.

Інституційний механізм управління в галузі забезпечення інформаційної безпеки держави, як пояснює Н. Грабар, є важливою структурною складовою державного апарату. Цей механізм спрямований на забезпечення виконання нормативних вимог та загальних правил поведінки, що регулюють взаємодію між різними економічними суб'єктами в інформаційному середовищі. Головною метою цього регулювання є попередження виникнення загроз для інформаційної безпеки держави [16].

Інституційний механізм управління у сфері забезпечення безпеки інформаційного простору держави є комплексною системою, спрямованою на організацію та координацію діяльності відповідальних органів публічної влади. Ці органи здійснюють заходи забезпечення інформаційної безпеки відповідно до чинного законодавства. Важливою складовою цього механізму є визначення шляхів його вдосконалення, що передбачає адаптацію до змін у зовнішньому середовищі та використання сучасних інформаційних технологій.

Ця система спрямована на досягнення високої ефективності заходів, спрямованих на протидію та попередження загроз інформаційній безпеці держави. Для успішного функціонування такого механізму необхідне не лише строге дотримання чинних законів та норм, але й гнучкість у реагуванні на швидкі зміни в технологічному ландшафті та інформаційному середовищі.

Отже, державна політика у сфері інформаційної безпеки охоплює широкий комплекс заходів і стратегій, спрямованих на захист інформаційної інфраструктури, ресурсів та простору від різноманітних загроз. Це включає регулювання, контроль і використання законодавчих та технічних інструментів для забезпечення конфіденційності, цілісності та доступності інформації. Також вона спрямована на боротьбу з

кіберзлочинністю, дезінформацією та підтримку цифрових прав та свобод громадян. Основна мета такої політики – управління реальними та потенційними загрозами для створення умов, які задовольняють інформаційні потреби людей і громадян, сприяючи реалізації національних інтересів. Система забезпечення інформаційної безпеки виступає як інструмент втілення такої політики та спрямована на досягнення цілей національної безпеки у сфері інформації.

Список використаних джерел

1. Інформаційна політика: навч. посібник / Г. Почепцов, С. Чукут. Київ: Знання, 2008. 663 с.
2. Коваль З. Політико-правові механізми державного управління інформаційно-психологічною безпекою України: автореф. дис. ... канд. н. з держ. упр., спеціальність: 25.00.02 – механізми державного управління. Одеса. 2011. 22 с.
3. Фомін В. Рось А. Сутність і співвідношення понять «інформаційна безпека», «інформаційна війна» та «інформаційна боротьба». *Наука і оборона*. 1999. № 4. С. 23–32.
4. Тертичка В. Державна політика: аналіз та здійснення в Україні: монографія. Київ: Основи, 2002. 750 с.
5. Дем'янчук О. «Державна політика» та «публічна політика»: варіант перехідного періоду. *Наукові записки. Політичні науки.* Національний університет «Києво-Могилянська академія». Київ, 2000. Т. 18. С. 31–36.
6. Шаповал Р., Клочко В. Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. *Наше право*. 2014. № 6. С. 5–9.
7. Кормич Б. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2003. 472 с.
8. Золотар О. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ Видавничий дім «АртЕк», 2018. 446 с.
9. Криштанович М. Механізми державної політики України щодо забезпечення національної безпеки. *Публічне управління та митне адміністрування*. 2019. № 3. С. 248–253.
10. Гаврильців М. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий журнал*. 2020. № 2. С. 200–203.
11. Палій С. Теоретичні засади функціонування державної політики у сфері інформаційної безпеки. *Публічне адміністрування та національна безпека.* 2019. № 6. URL: http://surl.li/snpba (дата звернення: 10.11.2023).
12. Архипова Є., Черниченко А. Забезпечення інформаційної безпеки в органах державної влади як нагальна потреба сьогодення. *Держава та регіони. Серія Державне управління.* 2018. № 4. С. 231–234.

13. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. *Ефективність державного управління*. 2015. Вип. 44. С. 13–20. URL: http://surl.li/snpbi (дата звернення: 11.032024).
14. Кириченко О. Концептуальні засади формування системи забезпечення інформаційної безпеки держави. *Вчені записки Університету «КРОК».* 2018. № 49. С. 19–26.
15. Федорчук О. Концептуальні засади формування системи забезпечення національної інформаційної безпеки. *Вісник соціально-економічних досліджень*, 2013. Вип. 2. С. 182–188.
16. Attacks against information systems: European Parliament legislative resolution, 4.07.2013. EUR-Lex: веб-сайт. URL: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013AP0321 (дата звернення: 04.04.2024).

В. Бортніков – доктор політичних наук,
професор кафедри політології та публічного управління ВНУ імені Лесі Українки

Політична участь (матеріали для лекції)

Політична участь *(*англ. – *political participation)*асоціюється із свідомими діями індивідів, спрямованими на захист своїх прав та інтересів, обстоюванням громадянських позицій, самоповагою та самореалізацією тощо. Поряд із категорією «політична участь» в науковому дискурсі використовують поняття «громадська участь», «громадська залученість», «громадянська активність», які, не виключаючи політичної складової із структури участі, акцентують увагу на її непрофесійному характері.

Уважне ставлення до феномену політичної участі пов’язано з розробленням концепції партисипативної (учасницької) демократії, що набула поширення в країнах Заходу в контексті пошуку альтернативних шляхів вдосконалення демократії. Теоретико-методологічні та емпіричні засади досліджень політичної участі обґрунтовані в працях Л. Мілбрата, С. Верби, Н. Ная, Г. Перрі, М. Каазе, А. Марша та ін. Праці Дж. Нагеля спрямовані на вивчення діяльнісного аспекту залучення в політику. Х. Макклоскі обґрунтовував психологічні аспекти політичної участі. Дж. Мойзер, Н. Дей здійснили аналіз неелекторальних типів