

КРУШЕНИЦЬКИЙ В. С.,
аспірант кафедри права
та правоохоронної діяльності
(Центральноукраїнський державний
університет імені Володимира
Винниченка)
ORCID ID: 0000-0001-9194-7897

УДК 351.746:004.738.5(477)
DOI <https://doi.org/10.32842/2078-3736/2023.3.88>

ПУБЛІЧНО-ІНФОРМАЦІЙНА СФЕРА ЯК СКЛАДОВА СИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У статті розглянуто публічно-інформаційну сферу як стратегічно важливу складову системи національної безпеки України в умовах глобалізації, цифровізації та гібридної війни. Автор підкреслює, що сучасне інформаційне середовище стало не лише каналом передачі знань і комунікації, а й об'єктом інформаційного протистояння, в якому зіштовхуються інтереси держав, корпорацій та окремих груп впливу. В умовах військової агресії з боку російської федерації публічно-інформаційна сфера набуває особливого значення як інструмент мобілізації суспільства, консолідації громадської думки та захисту національного суверенітету.

Увагу приділено правовим основам функціонування публічної інформації в Україні. Проаналізовано підходи до класифікації публічної інформації за ступенем доступності та наголошено на обов'язку органів державної влади забезпечувати прозорість та відкритість інформаційного обміну. Автор виокремлює публічно-інформаційну сферу як комплекс інституцій, процесів і технологій, через які здійснюється суспільна комунікація та реалізується інформаційна політика держави.

Окремо розглядаються ключові функції публічно-інформаційної сфери: інформаційно-комунікативна, аналітична, просвітницька, регулятивна та мобілізаційна. Автор стверджує, що ці функції мають безпосередній вплив на стан національної безпеки, адже забезпечують стійкість суспільства до дезінформації, сприяють формуванню критичного мислення, підвищенню інформаційної культури та національної ідентичності. Аналізуються актуальні загрози інформаційній безпеці, серед яких особливе місце займають інформаційні атаки, поширення фейкової інформації, кібератаки, втручання у державні інформаційні системи та маніпулювання громадською думкою.

У підсумку автор доходить висновку, що в Україні формується цілісна система інформаційної безпеки, до якої входять нормативно-правові акти (зокрема Доктрина інформаційної безпеки 2017 року, закони 2021–2022 років), інституційні структури (Центр стратегічних комунікацій при РНБО, Ситуаційний центр кібербезпеки при СБУ), а також просвітницькі ініціативи, орієнтовані на підвищення цифрової грамотності. В умовах сучасних викликів публічно-інформаційна сфера постає не лише як засіб комунікації, але й як арена боротьби за безпеку, стабільність і майбутнє демократичної України.

Ключові слова: публічно-інформаційна сфера, національна безпека, інформаційна політика, публічна інформація, дезінформація, стратегічні комунікації, кібербезпека, інформаційний суверенітет, доступ до інформації, гібридна війна, законодавче регулювання, інформаційна загроза, державна комунікація, критичне мислення, інформаційна культура.



Krushenitskyi V. S. Public information sphere as a component of the national security system of Ukraine

The article examines the public information sphere as a strategically important component of the national security system of Ukraine in the context of globalization, digitalization and hybrid warfare. The author emphasizes that the modern information environment has become not only a channel for the transfer of knowledge and communication, but also an object of information confrontation, in which the interests of states, corporations and individual groups of influence clash. In the context of military aggression by the Russian Federation, the public information sphere acquires special importance as a tool for mobilizing society, consolidating public opinion and protecting national sovereignty.

Attention is paid to the legal foundations of the functioning of public information in Ukraine. Approaches to the classification of public information by the degree of accessibility are analyzed and the obligation of state authorities to ensure transparency and openness of information exchange is emphasized. The author identifies the public information sphere as a complex of institutions, processes and technologies through which public communication is carried out and the state's information policy is implemented.

The key functions of the public information sphere are considered separately: informational and communicative, analytical, educational, regulatory and mobilization. The author argues that these functions have a direct impact on the state of national security, as they ensure the resistance of society to disinformation, contribute to the formation of critical thinking, increase information culture and national identity. Current threats to information security are analyzed, among which a special place is occupied by information attacks, the spread of fake information, cyberattacks, interference in state information systems and manipulation of public opinion.

As a result, the author concludes that a holistic information security system is being formed in Ukraine, which includes regulatory and legal acts (in particular, the Information Security Doctrine of 2017, laws of 2021–2022), institutional structures (the Center for Strategic Communications at the National Security and Defense Council, the Cybersecurity Situation Center at the SBU), as well as educational initiatives aimed at increasing digital literacy. In the context of modern challenges, the public information sphere appears not only as a means of communication, but also as an arena for the struggle for the security, stability and future of democratic Ukraine.

Key words: *public information sphere, national security, information policy, public information, disinformation, strategic communications, cybersecurity, information sovereignty, access to information, hybrid war, legislative regulation, information threat, state communication, critical thinking, information culture.*

Вступ. У сучасних умовах глобалізації та гібридних загроз, що постійно еволюціонують, особливого значення набуває публічно-інформаційна сфера як елемент національної безпеки України. Зростання впливу інформаційних технологій, соціальних медіа, цифрових комунікаційних каналів спричинило якісні зміни в механізмах впливу на суспільну свідомість. Інформація стала не лише інструментом, а й самостійним ресурсом протистояння у конфліктах нового типу – інформаційних війнах.

На фоні збройної агресії російської федерації проти України, особливої актуальності набуває проблема захисту інформаційного простору держави. Пропаганда, дезінформація, маніпулятивні впливи, кібератаки та підривна діяльність у медіа-просторі загрожують стабільності політичної системи, громадській згоді, а також державному суверенітету. Водночас, відсутність ефективної координації між органами державної влади у сфері інформа-



ційної політики, недостатній рівень інформаційної культури населення та низький рівень медіаграмотності ускладнюють реагування на ці виклики.

Таким чином, актуальність дослідження зумовлена необхідністю визначення місця та ролі публічно-інформаційної сфери в структурі національної безпеки, обґрунтування механізмів її регулювання, а також розробки стратегічних підходів до формування сталого, безпечного інформаційного середовища.

Питання публічно-інформаційної сфери як складової системи національної безпеки України неодноразово привертало увагу вчених. Так, можна виділити наступних дослідників: О. М. Бандурка, І. Р. Березовська, В. В. Василевич, Б. М. Головкін, С. О. Гнатюк, В. І. Гур'єв, О. П. Дзьобань, Б. А. Кормич, В. В. Марков, В. С. Цимбалюк, О. К. Юдін та інші.

Постановка завдання. Метою статті є теоретичне обґрунтування ролі публічно-інформаційної сфери як стратегічного чинника у забезпеченні національної безпеки України.

Результати дослідження. Публічно-інформаційна сфера в сучасному глобалізованому середовищі перетворилась на одну з найважливіших складових національної безпеки. Її стратегічна значущість посилилася на тлі новітніх інформаційних технологій, зростання ролі соціальних мереж, масового поширення цифрового контенту, а також в умовах гібридної війни, яку проти України веде російська федерація. У зв'язку з цим виникає потреба глибокого переосмислення ролі та функцій інформаційного простору в забезпеченні державного суверенітету, стабільності й цілісності країни. Від ефективного функціонування публічно-інформаційної сфери залежить не лише об'єктивність суспільного сприйняття подій, а й рівень консолідації громадян, стійкість до ворожих впливів та здатність держави формувати і підтримувати національні цінності.

Першочергово доцільно зупинитися на концептуалізації поняття публічної інформації в сучасному правовому полі. У цьому контексті заслуговує на увагу дослідження Е. Аблякімової, яка наголошує, що категорія «публічна інформація» охоплює широкий спектр інформації незалежно від її змістового наповнення [1, с. 53]. Відповідно до положень статті 10 Закону України «Про інформацію» [2], до публічної інформації можуть належати: інформація про фізичну особу, довідково-енциклопедична інформація, екологічна інформація, дані про товари, роботи чи послуги, науково-технічна, податкова, правова, статистична, соціологічна інформація тощо – тобто будь-яка інформація, що може надаватися за запитами зацікавлених осіб [1, с. 53].

Крім того, відповідно до змісту статті 6 Закону України «Про доступ до публічної інформації», класифікація публічної інформації може здійснюватися за критерієм доступності: вона поділяється на відкриту, конфіденційну, таємну та службову. Особливий інтерес становить також те, що в окремих випадках поняття публічної інформації може включати й масову інформацію – за умови забезпечення доступу до неї шляхом систематичного та оперативного оприлюднення, як це передбачено частиною першою статті 5 згаданого Закону. Таке нормативне визначення зумовлено передусім прагненням законодавця створити ефективний механізм реалізації права на доступ до інформації [3; 1, с. 54].

Варто підкреслити, що ключовим чинником, який дозволяє віднести ту чи іншу інформацію до категорії публічної, є наявність у спеціально уповноважених суб'єктів – зокрема, органів державної влади та інших розпорядників інформації – обов'язку забезпечити доступ до неї. Саме цей функціональний аспект є підставою для виділення публічної інформації як окремої правової категорії у системі інформаційних правовідносин [1, с. 54].

Відповідно до ст. 1 Закону України «Про доступ до публічної інформації» (далі – Закон № 2939-VI) публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом [3].

Таким чином, публічно-інформаційна сфера – це сукупність інформаційних потоків, інститутів і засобів комунікації, через які здійснюється інформування, взаємодія та вплив



на суспільство. Вона включає як традиційні засоби масової інформації – телебачення, радіо, пресу, – так і цифрові канали: соціальні мережі, онлайн-медіа, месенджери, форуми, відеоплатформи. Державна влада, громадянське суспільство, освітні та наукові інститути, приватні медіа – всі ці суб'єкти формують інформаційне середовище, в якому циркулюють ідеї, думки, факти, оцінки. Однією з головних особливостей сучасного етапу розвитку інформаційного простору є його відкритість, динамічність, технічна складність і високий рівень взаємопов'язаності між глобальним і національним контекстом.

Публічно-інформаційна сфера виконує низку функцій, які мають безпосередній вплив на стан національної безпеки. По-перше, вона забезпечує інформування населення про дії органів влади, події в країні та світі. По-друге, формує громадську думку, що прямо впливає на легітимність державної влади. По-третє, бере участь у мобілізації суспільства в умовах криз, надзвичайних ситуацій або воєнної агресії. По-четверте, виконує освітню функцію, формуючи критичне мислення, рівень медіаграмотності та інформаційну культуру громадян. Нарешті, вона слугує майданчиком для діалогу, конкуренції ідей та контролю за владою, що є необхідним елементом демократії.

Серед основних функцій можна виокремити інформаційно-комунікативну, аналітичну, просвітницько-виховну, регулятивну та мобілізаційну. Інформаційно-комунікативна функція забезпечує зв'язок між суб'єктами владних повноважень та громадськістю, формує відкритість і підзвітність державної влади [4, с. 16]. Аналітична функція полягає у зборі, систематизації та інтерпретації суспільно значущої інформації, що дозволяє оперативно реагувати на потенційні загрози, оскільки на сьогодні в Україні інформаційно-аналітична діяльність здебільшого спрямована на розробку нових та вдосконалення вже існуючих баз даних. Це поширюється як на всіх громадян, так і на державні органи. Просвітницько-виховна функція сприяє підвищенню рівня інформаційної культури населення, формуванню патріотичної свідомості та стійкості до деструктивних інформаційних впливів.

Регулятивна функція реалізується через систему законодавчих і підзаконних актів, які регламентують доступ до інформації, її використання, захист персональних даних, а також протидію пропаганді та дезінформації. Мобілізаційна функція публічно-інформаційної сфери проявляється у здатності консолідувати суспільство в умовах криз або зовнішньої загрози, сприяти збереженню суспільної стабільності та підтримці обороноздатності держави. Усі зазначені функції є взаємопов'язаними та забезпечують цілісність інформаційної політики держави як невід'ємного елементу системи національної безпеки.

Разом із тим, інформаційна сфера є об'єктом і середовищем, у якому здійснюються численні загрози.

Загрози інформаційній безпеці, це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особи, суспільства й держави в інформаційній сфері [5, с. 19].

У своєму навчальному посібнику В. Гур'єв, Д. Мехед, Ю. Ткач, І. Фірсова, акцентують увагу, що основні загрози інформаційній безпеці можна поділити на три групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особу, суспільство, державу;
- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію й інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);
- загрози інформаційним правам і свободам особи (праву на виробництво, поширення, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на захист честі й гідності тощо) [5, с. 19].

Таким, чином, загроза інформаційній безпеці – це потенційна можливість порушення режиму інформаційної безпеки. Навмисна реалізація загрози називається атакою на інформаційну систему. Особи, які навмисно реалізують загрози, є зловмисниками. Найчастіше загроза є наслідком наявності вразливих місць у захисті інформаційних систем, наприклад, неконтрольований доступ до персональних комп'ютерів або неліцензійне програмне забезпечення (на жаль, навіть ліцензійне програмне забезпечення не позбавлене вразливостей) [5, с. 19].



З 2014 року Україна є об'єктом масованої інформаційної агресії з боку російської федерації. Основними її елементами є: систематичне поширення фейкової інформації, маніпуляції фактами, використання історичних наративів для створення антиукраїнських образів, дискредитація Збройних Сил України, розпалювання ворожнечі між регіонами, провокування протестів і недовіри до інституцій. Особливо небезпечним є використання технологій глибинного фейку, бот-мереж, автоматизованих систем впливу на алгоритми соціальних мереж, а також створення альтернативної картини реальності шляхом постійного інформаційного тиску.

У цьому контексті Україна була змушена активно розвивати нормативно-правову, інституційну та технологічну складову системи інформаційної безпеки. У 2017 році було прийнято Доктрину інформаційної безпеки, яка визначила основні загрози та пріоритети державної політики у цій сфері.

У документі йдеться про національні інтереси України в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці, пріоритети державної політики в інформаційній сфері і механізм реалізації доктрини [6].

Втілювати положення повинні Кабінет міністрів, Міністерство інформаційної політики, Міністерство закордонних справ, Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Служба безпеки України, розвідувальні органи, Державна служба спеціального зв'язку та захисту інформації, Національний інститут стратегічних досліджень; передбачаються також законодавчі зміни, а отже – парламент [6].

Серед положень доктрини є як захист українського суспільства від «агресивного інформаційного впливу російської федерації», так і розвиток публічної дипломатії, в тому числі культурної та цифрової; як видалення інформації з українського сегменту інтернету, так і квотування національного аудіовізуального контенту; як захист права на вільний доступ до інформації, так і створення механізмів захисту від пропаганди та багато іншого [6].

Також, було прийнято законодавчі ініціативи 2021–2022 років, зокрема Закон України «Про основи національного спротиву» [7], а також новий Закон України «Про медіа» [8], суттєво розширили повноваження державних органів у протидії ворожому впливу.

Важливим кроком є створення Центру стратегічних комунікацій та інформаційної безпеки при РНБО. Він виступає своєрідним державним механізмом протидії дезінформації, що дозволяє захищати інформаційний простір від викривлень та вкидів. Центру стратегічних комунікацій та інформаційної безпеки спрямований на об'єднання зусиль громадських організацій та влади у боротьбі із дезінформацією, швидке реагування на фейки, а також на промочію українських наративів [9].

Особливу увагу слід приділити питанню кібербезпеки, яка є технічною основою для захисту інформаційної сфери. Кібератаки на об'єкти критичної інфраструктури, медіа, державні сайти, освітні платформи, мобільні додатки стали звичним явищем, що вимагає постійної модернізації захисних систем. Україна, у співпраці з НАТО, Європейським Союзом та окремими державами, активно розбудовує кіберрезерв, системи раннього виявлення загроз, аналітичні центри обробки інформації та реагування. Паралельно з технічним захистом розвиваються механізми правового регулювання у сфері цифрової безпеки, персональних даних, свободи вираження в інтернеті.

Починаючи з 2018 року розпочав свою роботу Ситуаційний центр забезпечення кібербезпеки при Службі безпеки України. Цей уряд створився при допомозі Північноатлантичного альянсу. Технічне обладнання і програмне забезпечення діяльності Центру було надано в межах здійснення першого рівня Угоди про здійснення Трастового фонду України – НАТО щодо питань кібербезпеки. На основі Ситуаційного центру, сформувалась система управління подіями інформаційної безпеки. Це надає можливість швидко виявляти, реагувати і прогнозувати загрози в сфері національного кіберпростору [10, с. 403].

Також, для системної протидії інформаційним та цифровим викликам уряд України схвалив Стратегію інформаційної безпеки до 2025 р. Метою Стратегії є протидія внутрішнім та зовнішнім загрозам, підтримка інформаційними засобами соціальної і політичної стабільності й оборони держави [11].



Таким чином, Україна послідовно розвиває свою стійкість до дезінформаційних загроз, формуючи комплексну систему інформаційної безпеки, що охоплює як нормативно-правові механізми, так і розвиток цифрової грамотності, стратегічних комунікацій та кіберзахисту, що в сукупності дозволяє ефективно реагувати на виклики гібридної війни та зберігати інформаційний суверенітет. Оскільки, інформаційний суверенітет — це ще один ключовий концепт, без якого неможливо уявити повноцінне функціонування держави. Він включає право і спроможність держави формувати власну інформаційну політику, розвивати національний медіа-простір, забезпечувати мовну, культурну та технологічну самостійність. У цьому сенсі надзвичайно важливим є розвиток україномовного контенту, підтримка незалежних ЗМІ, боротьба з монополізацією ринку інформації та дотримання балансу між свободою слова і безпекою.

Публічно-інформаційна сфера також тісно пов'язана з гуманітарною та освітньою політикою держави. Формування національної ідентичності, патріотичного світогляду, критичного мислення, а також виховання толерантності, поваги до прав людини та демократичних цінностей починається з доступу до якісної, достовірної та різноманітної інформації. Тому державна підтримка систем медіаосвіти, інтеграція курсів із медіаграмотності у шкільну та вищу освіту, створення національних платформ фактчекінгу і журналістських розслідувань є не менш важливими, ніж розвиток технічних засобів захисту.

Висновки. Отже, публічно-інформаційна сфера виступає як одночасно джерело сили і потенційної уразливості. У руках відповідальних державних інституцій, незалежних медіа та свідомих громадян вона стає інструментом зміцнення демократичних основ, національної єдності та стійкості перед зовнішніми загрозами. У разі ж нехтування її значенням або монополізації вона може бути використана для деструктивного впливу на свідомість суспільства, знищення легітимності влади та дестабілізації держави. Тому ключовим викликом для України є не лише оборона, а й активне формування, стратегічне управління та постійне оновлення інформаційного середовища, яке відповідатиме інтересам національної безпеки, розвитку і самостійності держави.

Список використаних джерел:

1. Аблякімова Е. Е. Правове і суспільне значення публічної інформації. *Актуальні проблеми політики*. 2013. Вип. 50. С. 52-60.
2. Про інформацію: Закон України від 02 жовтня 1992 р. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12/ed20230727#Text>
3. Про доступ до публічної інформації: Закон України від 13 січня 2011 р. № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17/ed20110113#Text>
4. Малімон В.І. Комунікативні технології в публічному управлінні: навчально-методичні матеріали. Івано-Франківськ, ІФОЦППК, 2018. 51 с.
5. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с. : іл.
6. Доктрина інформаційної безпеки України – це лише декларація – експерти. URL: <https://www.radiosvoboda.org/a/28336852.html>
7. Про основи національного спротиву: Закон України від 16 липня 2021 р. 1702-IX. URL: <https://zakon.rada.gov.ua/laws/show/1702-20#Text>
8. Про медіа: Закон України від 13 грудня 2022 р. 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>
9. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. URL: <https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki>
10. Колосовський Є.Ю., Круць Е.М. Сучасний стан кібербезпеки України в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. №12. С. 402-405
11. Кібербезпека й медіаграмотність: Україна на передовій інформаційного фронту. URL: <https://adastra.org.ua/blog/kiberbezpeka-j-mediagramotnist-ukrayina-na-peredovij-informacijnogo-frontu>

