

УДК 347.43

DOI <https://doi.org/10.32840/pdu.2022.1.23>

А. В. Миколіук

кандидат політичних наук,
асистент кафедри

Навчально-наукового інституту публічного управління
та державної служби Київського національного університету
імені Тараса Шевченка

ПУБЛІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: ДІДЖИТАЛІЗАЦІЯ ТА ІНФОРМАЦІЙНА ВІЙНА

Розвиток сучасної держави, як суверенного, демократичного, правового суб'єкту потребує створення стабільної та надійної безпекової системи, яка б могла захистити її від зовнішніх посягань а внутрішніх диверсій. Звісно, поняття безпеки має різні форми і в кожній сфері забезпечується за рахунок іншого набору інструментів. Проте, можна точно стверджувати, що одним з ключових в цій темі сьогодні постає питання інформаційної безпеки. Особливо ця тема актуалізується в контексті активного розвитку процесів діджиталізації та переведення все більшого сегменту публічного управління в цифровий вимір. Крім того, загострює необхідність дослідження цього питання ще й гібридна війна, яка вже не перший рік ведеться проти нашої держави в інформаційному полі, а наразі перейша у фазу ескалації.

Зазначені фактори дозволяють нам стверджувати, що Інформаційна безпека сьогодні є першочерговою сферою відповідальності сучасної держави. Побудова стабільної та сучасної інформаційної політики дозволяє країні захищати власні інтереси, протистояти загрозам (внутрішнім та зовнішнім). В Україні інформаційна політика є складовою соціально-економічної політики.

Наразі назріла необхідність у вдосконаленні публічного управління інформаційною безпекою держави. В цьому процесі варто враховувати низку об'єктивних чинників: політико-економічну та геополітичну ситуацію в світі, загальну тенденцію до діджиталізації в ключових сферах, розвиток інформаційних технологій та необхідності захищати власні національні інтереси в умовах ведення активної інформаційної війни з країною-агресором. Відповідно, забезпечення інформаційної безпеки, сьогодні потребує додаткового теоретичного дослідження та якнайшвидшого законодавчого врегулювання окремих проблемних моментів.

Проте, при успішному реформуванні, збалансована система публічного управління інформаційною безпекою для України може стати гарантією подальшого успішного розвитку в умовах тотальної діджиталізації всіх сфер.

Ключові слова: інформаційна безпека, інформація, публічне управління, діджиталізація, інформаційна війна.

Постановка проблеми. Перш за все, варто визначити, що ми маємо на увазі під поняттям «інформаційна безпека». Одне з найбільш вичерпних визначень, яке підходить нам в контексті дослідження, інформаційна безпека – це поєднання внутрішніх і зовнішніх аспектів національної безпеки, що має на меті захист інтелектуальної власності господарюючих суб'єктів і громадян, охорону та примноження культурного надбання країни, а також збереження відомостей, що становлять державну і професійну таємницю.

Сьогодні розвиток будь-якої демократичної держави можливий лише за умови забезпечення інформаційної безпеки всіх суб'єктів інформаційних відносин. Рівень розвитку та безпеки інформаційного простору країни є системоутворюючими факторами у забезпеченні безпеки, що активно впливають на стан політичної, економічної, соціальної, воєнної, інформаційної та інших складових частин національної безпеки держави.

Зауважимо, що сьогодні існує певна напруженість в пошуку ідеального співвідношення між концепцією прозорості публіч-

ного управління і необхідністю захисту суспільно значущої інформації. При тому, що будь-яка демократична держава має прагнути до створення системи масимальної прозорості дій та відкритості інформації, існують ситуації, коли уряди вимушено захищають окремі види інформації із міркувань національної безпеки. Причини та аргументація для цього може різнитись в залежності від типу політичного режиму в країні. Проте, зміни в державній інформаційній політиці і механізмах її втілення можуть відбуватись не лише під впливом політичного режиму, на цей процес впливає безлічі акторів і багато залежить від того, які суб'єкти мають найбільший вплив на даний момент.

Враховуючи багатогранність та складність публічного управління інформаційною безпекою, не можна не відмітити актуалізацію даного питання у зв'язку з розгортанням активної фази гібридної інформаційної війни та нагальній потребі в подальшій теоретичній розробці даної теми.

Аналіз останніх досліджень і публікацій. Проблема інформаційної політики та інформаційної безпеки є предметом дослідження багатьох вітчизняних і зарубіжних учених І. Арістової, А. Марущака, Ю. Нисневича, Г. Почепцова, В. Петрика, В. Ліпкана, Б. Кормича, В. Почепцова та інших. Зазвичай ці дослідження мають багатовекторний характер і здійснюються в різних напрямках (створення нових і модернізація існуючих технічних засобів передачі, накопичення, зберігання та захисту інформації, розробка нових інформаційних технологій та програмних продуктів, формування ефективної нормативно-правової бази для регламентації дій в інформаційному просторі і напрацювання дієвих механізмів протидії деструктивним проявам). Наразі фактично відсутні комплексні дослідження, які б давали нам вичерпне уявлення про можливість удосконалення публічного управління інформаційною безпекою в умовах війни та діджиталізації.

Мета статті – визначити пріоритетні напрями розвитку публічного управління інформаційної політики для ефективного функціонування в умовах інформаційної війни з агресором та підтримки безпеки під впливом процесів діджиталізації.

Виклад основного матеріалу. Сьогодні ми можемо спостерігати активне розгортання двох взаємопов'язаних процесів: зростання ролі інформації в житті людей, збільшення її обсягів та урізноманітнення форм, та розвиток і вдосконалення технологій, їх інтеграцію в наше повсякденне життя. Це дає нам підстави говорити про настання так званої «інформаційної революції», яка суттєво збільшує роль інформаційного фактору в процесі суспільного розвитку [6, с. 91].

Зазначені процеси перетворюють сферу інформації в пріоритетну галузь життєдіяльності суспільства і, відповідно, в один з ключових об'єктів державного управління. На жаль, на сьогоднішній день в українському законодавстві відсутнє чітке визначення терміну «інформаційна сфера», як і перелік її основних компонентів. Закон України «Про інформацію» в своїй статті 3 частково окреслює виключно рамки інформаційної сфери. В тексті вказано, що «дія закону поширюється на інформаційні відносини, які виникають у всіх сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації» [4].

В той же час, закон України «Про Концепцію державної інформаційної політики» містить більш вичерпне трактування інформаційної сфери: «сукупність інформаційних ресурсів, інформаційної інфраструктури, суб'єктів інформаційних відносин, які забезпечують збирання, зберігання, використання та поширення інформації, а також системи правового регулювання суспільних відносин у цій сфері й організації виробництва засобів» [9].

Відсутність чіткого нормативно-правового забезпечення говорить ще й про складність створення дієвої системи державного управління для інформаційної сфери. Динамічність цієї сфери, адаптивність та високі темпи розвитку та змін просто не дають можливість державі завжди оперативно реагувати на нові інформаційні явища та процеси за використанням управлінських засобів.

Наразі державне управління інформаційною сферою носить галузевий характер. На думку дослідника Б. Курашвілі, даний різновид управління має включати 8 функцій:

- «організація системи і процесу управління;
- маркетинг і ринок продукції галузі;
- визначення та реалізація політики і стратегії розвитку галузі;
- управління розвитком інфраструктури галузі;
- забезпечення розвитку науково-технічного потенціалу галузі;
- ситуаційне управління структурами галузі;
- мобілізація та використання ресурсів галузі;
- управління інвестиціями, розвитком робочих місць і підготовкою кадрів» [7, с. 72].

В свою чергу, І. Арістова в своїй роботі зазначає, що в основі державної інформаційної політики України лежить прагнення сформувавши відкрите інформаційне суспільство. Його основою мають стати:

- урахування національних особливостей і інтересів;
- прагнення до інтеграції у світовий інформаційний простір;
- єдиний інформаційний простору цілісної держави;
- забезпечення інформаційної безпеки на внутрішньодержавному та міжнародному рівнях [8].

Дослідник Г. Почепцов в своїх працях стверджує, що особливу увагу варто приділяти інформаційній безпеці, яка є основним аспектом інформаційної політики [1]. Для побудови дієвої системи інформаційної безпеки, варто зрозуміти, наскільки чинна система публічного управління має можливість відповідати на сучасні поточні виклики, що викликані діджиталізацією. Крім того, варто визначити, чи відповідають потребам системи державного управління сучасні інформаційно-телекомунікаційні системи.

Нова модель публічного управління має бути сформована на основі електронних платформ, які стають її технічною основою, вони є відкритими та технічно нейтральними, що дозволяє вільно обмінюватися ресурсами. Платформа має свій набір інструментарію, який дозволяє визначити характеристики аудиторії, поширювати контент, обрати спосіб підключення та взаємодії учасників.

Завданням кожної розвиненої країни сьогодні є вироблення власної дієвої державної інформаційної політики, яка б враховувала всі вищезгадані аспекти. Державна інформаційна політика – «це політика, яка засобами державної влади створює і забезпечує функціонування системи правового регулювання інформаційних відносин, захист прав і основних свобод людини, збалансованість інтересів людини, суспільства і держави у всіх сферах інформаційної діяльності» [2].

Варто зауважити, що попри загальносвітову тенденцію впровадження відкритих даних та відкритого доступу до інформації, позиція урядів щодо цього питання в контексті розробки інформаційної політики може різнитись. І, якщо в авторитарних країнах цей процес є суворо централізованим та підконтрольним, а отже сфери «доступу» до інформації визначені чітко та однозначно, то в умовах демократії до цього процесу залучена величезна кількість суб'єктів, що створює ситуацію напруженості та дискусійності, адже потрібно знайти баланс між відкритістю та безпекою.

Окрім вчені дійшли висновку, що демократія неодмінно втрачає заявлені цінності «прозорості» при виникненні серйозної загрози національної безпеки. Потреба в захисті наближує демократичний та авторитарний підходи в цій сфері, зміщуючи акценти в бік централізованості та керованості [21; 19].

Це приводить нас до внутрішнього конфлікту, який все більше загострюється з розвитком глобальної мережі Інтернет – повна прозорість демократичних норм ап'орі протиставляється державній таємниці та секретністю, яка необхідна для певних галузей і в якій може бути зацікавлена виконавча влада. Проте, враховуючи останні події в політичній та геополітичній сферах, рівень конфліктів та загальносвітової напруженості, можна стверджувати, що сьогодні більшість урядів схиляються на бік безпеки критично важливої інформації, а не її поширення [20]. Так, наприклад, переглядається доцільність виведення у відкритий доступ інформації про переміщення озброєння, яка раніше в ряду країн публікувалась у електронній звітності.

Формування державної інформаційної політики та створення достатніх умов для її подальшої реалізації сьогодні є основою ефективного управління інформаційним суспільством, що потребує узгодження системно-функціональної та інформаційної складових. Що особливо актуалізується під впливом активного розвитку процесів діджиталізації в більшості сфер. Правову основу інформаційної безпеки держави в Україні формує інформаційне законодавство. На сьогоднішній день ми маємо вже доволі розвинену систему нормативно-правових актів, що мають на меті регулювання суспільних відносин в інформаційній сфері (електронне законодавство), що забезпечує «регулювання суспільних інформаційних відносин у процесі збору, реєстрації, накопичення, зберігання, використання та поширення даних (обробка даних), а також захист інформаційних ресурсів (продуктів, технологій), які здійснюються за допомогою інформаційно-комп'ютерних технологій та телекомунікаційних мереж» [17; 3].

Окремі питання державної інформаційної політики та діяльності щодо забезпечення інформаційної безпеки регулюють:

Закони України:

- «Про захист інформації в інформаційно-телекомунікаційних системах»;
- «Про інформаційні агентства»;
- «Про авторське право і суміжні права»;
- «Про друковані засоби масової інформації (пресу) в Україні»;
- «Про телебачення і радіомовлення»;
- «Про розповсюдження примірників аудіовізуальних творів та фонограм».

Укази Президента України:

- «Про Стратегію національної безпеки України»;
- «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні»;

Постанова Кабінету Міністрів України:

- «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [10; 12; 13; 14; 15; 16].

Сьогоднішні реалії загострення гібридної війни в інформаційному полі суттєво

підвищили актуальність питання вдосконалення кібербезпеки України. І, хоч в цьому напрямку вже було впроваджено ряд позитивних змін (затверджена «Стратегія кібербезпеки України», прийнятий Закон «Про основні засади забезпечення кібербезпеки України», ратифіковано міжнародну «Конвенцію про кіберзлочинність» [5; 11; 18]), проте необхідно продовжувати рух в цьому напрямку.

Крім того, варто працювати над розвитком інформаційного суспільства в Україні, адже воно є базою для впровадження ефективної інформаційної політики держави. І для цього необхідно вдосконалити застарілу нормативно-правову базу в інформаційній сфері, постійно підвищувати рівень комп'ютерної та інформаційної грамотності населення, активно працювати над впровадженням новітніх методів навчання та забезпечити загальний доступ населення до мережі Інтернет. Робота в цьому напрямку наразі вже ведеться, але її темпи все ще є недостатніми для підтримки конкурентоспроможності держави в цій сфері.

Висновки і пропозиції. Проблеми інформаційної безпеки на сьогодні актуалізуються значним зростанням ролі та обсягів інформації, в останні роки суттєво збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації. Саме тому, одним з ключових пріоритетів держави стає інформаційна безпека. Особливо це питання актуалізується на фоні загострення гібридної інформаційної війни яку вже багато років ведуть проти нашої держави. Тому наразі важливо комплексно та активно вирішувати проблеми, пов'язані із забезпеченням інформаційної безпеки.

Ключовим пріоритетом сьогодні залишається, створення цілісної системи у вигляді Інформаційного кодексу. Це дозволить структурувати та узгодити наявний масив нормативно-правових актів, що регламентують забезпечення інформаційну безпеку. Адже наразі між ними спостерігається концептуальна і термінологічна неузгодженість, крім того, все ще діють застарілі та неефективні норми. Також, важливо постійно підвищувати рівень комп'ютерної та інформаційної грамотності населення, активно працювати

над впровадженням новітніх методів навчання та забезпечити загальний доступ населення до мережі Інтернет.

Список використаної літератури:

1. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти: монографія / за ред. О. М. Бандурки. Харків : Ун-ту внутр. справ, 2000. 368 с.
2. Арістова І. В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія. Харків : Нац. ун-т внутр. справ, 2006. 354 с.
3. Забезпечення інформаційної безпеки як функція сучасної держави : монографія / Тихомиров О. О. ; заг. ред. Р. А. Калюжний. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.
4. Закон України «Про інформацію». *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.
5. Конвенція про кіберзлочинність : ратифікація 07 вер. 2005 р. : Рада Європи; Конвенція, Міжнародний документ від 23 лист. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 16.10.2021).
6. Нисневич Ю. А. Информационный фактор политической модернизации. *Вестник Московского университета. Сер. 12. Политические науки*. 2001. С. 89–94.
7. Курашвили Б. П. Очерк теории государственного управления. М., 1987. 292 с.
8. Почепцов Г. Г., Чукут С. А. Інформаційна політика : навч. посіб. Київ : Знання, 2006. 663 с.
9. Проект Закону України «Про Концепцію національної інформаційної політики України». URL: // www.rada.kiev.ua
10. Про Концепцію Національної програми інформатизації : Закон України від 07 лип. 2011 р. № 3610-VI. *Відомості Верховної Ради України*. 2012. № 7. Ст. 53.
11. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. 2017. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 16.10.2021).
12. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09 січ. 2007 р. № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.
13. Про рішення Ради національної безпеки і оборони України від 14 вер. 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 вер. 2020 р. № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text> (дата звернення: 16.10.2021).
14. Про рішення Ради національної безпеки і оборони України від 6 трав. 2015 року «Про Стратегію національної безпеки України» : Указ Президента України від 26 травня 2015 р. № 287/2015. URL: <http://zakon4.rada.gov.ua/laws/show/287/2015/paran7#n7> (дата звернення: 16.10.2021).
15. Про Стратегію національної безпеки України: Указ Президента України від 12 лют. 2007 р. № 105/2007. URL: <http://zakon1.rada.gov.ua/laws/show/105/2007> (дата звернення: 16.10.2021).
16. Скулиш Є., Прокоф'єва Д. Безпека кіберпростору як елемент національної безпеки в умовах глобалізації інформаційних процесів. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2007. Вип. 2(15). С. 26–31.
17. Старіш О. Г. Інформаційна політика держави в контексті глобалізації : дис. ... д-ра політ. наук : 23.00.16 / Київський національний університет ім. Т. Шевченка. Київ, 2008. 401 с.
18. Житко А. О. Кібервійна як складова гібридної війни. *Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення* : матеріали Всеукр. наук.-практ. конф. / Маріуполь : ДонДУУ. 2017. С. 263–266.
19. Anderson J. Public policymaking. Boston : Wadsworth Publishing. 2011.
20. McChesney R. W. The Internet and U. S. communication policy-making in historical and critical perspective. *Journal of Communication*. 1996. V. 46. P. 98–124.
21. Rosenzweig P. Cyber warfare: How conflicts in cyberspace are challenging America and changing the world. Westport, CT : Praeger Publishers, 2013.

Mikolyuk A. Public management of information security: digitalization and information warfare

The development of the modern state, as a sovereign, democratic, legal entity, requires the creation of a stable and reliable security system that could protect it from external encroachments and internal sabotage. Of course, the concept of security has different forms and in each area is provided by a different set of tools. However, it is safe to say that one

of the key issues in this topic today is information security. This topic is especially relevant in the context of the active development of digitalization and the transformation of a growing segment of public administration in the digital dimension. In addition, the need to study this issue is exacerbated by the hybrid war, which has been waged against our state for more than a year in the information field, but is now entering an escalation phase.

These factors allow us to say that information security today is the primary area of responsibility of the modern state. Building a stable and modern information policy allows the country to protect its own interests, resist threats (internal and external). In Ukraine, information policy is a component of socio-economic policy.

Now there is a need to improve the public management of information security of the state. This process should take into account a number of objective factors: the political, economic and geopolitical situation in the world, the general trend towards digitalisation in key areas, the development of information technology and the need to protect national interests in an active information war with the aggressor country. Accordingly, the provision of information security today requires additional theoretical research and the earliest possible legislative settlement of certain issues.

However, with successful reform, a balanced system of public information security management for Ukraine can be a guarantee of further successful development in the context of total digitalization of all spheres.

Key words: *information security, information, public administration, digitalization, information war.*