УДК 351.751+004.056.5(477)

Глобенко Сергій

ORCID iD 0000-0002-9751-4213
e-mail: svhlobenko@ukr.net

ІНФОРМАЦІЙНИЙ ПРОСТІР ДЕРЖАВИ ТА ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЙОГО ЗАХИСТУ В УКРАЇНІ

https://doi.org/10.33269/2618-0065-2023-1(13)-195-210

Анотація. З урахуванням мінливого й швидко змінюваного середовища охарактеризовано основні підходи держави до забезпечення ефективної побудови та стабільного функціонування її інформаційного простору, що в нинішніх умовах набуває особливо важливого, концептуального значення. Досліджено проблематику державної політики в інформаційній сфері з акцентом на гарантуванні інформаційної безпеки, значний інтерес до якої продиктований сучасною суспільною дійсністю. Розглянуто погляди щодо забезпечення національної безпеки і оборони держави в умовах новітніх загроз і викликів в аспекті необхідності досягнення максимально можливої стійкості як окремих її складових, так і самої системи в цілому, що зумовлено складними умовами її нинішнього функціонування і потребою її подальшого збереження. Виокремлено особливості національного інформаційного простору та з'ясовано основні проблеми його подальшого розвитку з урахуванням забезпечення безпеки особи, суспільства, держави як одного із основоположних факторів функціонування механізму держави, який характеризується значним рівнем комплексності й багатоаспектності, що нині в умовах України потребує пошуку максимально ефективних управлінських рішень. Проаналізовано роль і місце України у загальносвітових рейтингах безпекових спроможностей у сфері захисту інформаційного простору, відповідних механізмів державного управління, а також основних чинників, які впливають на ці процеси. Узагальнено й систематизовано фактори формування державної системи інформаційної безпеки, напрями імплементації стратегічних планів та відповідних заходів з питань забезпечення безпеки в інформаційній сфері в умовах надзвичайних і кризових явищ, наведено теоретичні й прикладні аспекти перспектив подальшого розвитку інформаційного простору держави і забезпечення його захисту в умовах України.

Ключові слова: інформаційний простір держави, інформаційна безпека, захист інформаційного простору, державна політика в інформаційній сфері, механізми державного управління.

Постановка проблеми. Проблеми, пов'язані з інформаційним простором держави, перебувають у центрі уваги

всіх держав світу, адже виклики й загрози у цій сфері проявляються у прямому, опосередкованому чи ймовірнісному аспекті і позначаються як на системі національної безпеки загалом, так і на окремій її складовій. У цьому контексті забезпечення безпеки особи, суспільства, держави набуває особливо важливого, концептуального значення через взаємозалежність, за якої неврахування окремих аспектів кожної складової може призвести до негативних наслідків для усього механізму держави. Разом із тим забезпечення інформаційної безпеки держави має безпосередній вплив на забезпечення як національної безпеки загалом, так і окремих її компонентів.

Аналіз останніх досліджень і публікацій. Матеріали нашого дослідження ґрунтуються на працях, дотичних до проблем забезпечення національної безпеки загалом та інформаційної безпеки зокрема. Так, О. Резнікова [1], досліджуючи теоретичні й прикладні аспекти національної стійкості України, пропонує низку рекомендацій концептуального характеру й обґрунтовує авторське бачення моделі її побудови, підходи щодо формування й реалізації відповідної комплексної державної політики у цій сфері в нашій країні. О. Кантур [2] обґрунтовано доводить, що в умовах воєнних дій Україна демонструє найвищий ступінь стійкості до проявів дезінформації в медіапросторі, виявляючи тим самим власну спроможність протистояти іноземним інформаційним загрозам. Р. Прав [3], характеризуючи механізми формування і реалізації політики державної безпеки в інформаційній сфері, наголошує на доцільності застосування інноваційних підходів у разі виявлення та ідентифікації загроз, пропонує практичні рекомендації й визначає пріоритетні завдання з метою підтримання належного рівня безпеки в окресленій сфері. В. Торічний [4] розглядає проблеми інформаційного забезпечення безпеки держави в системі національної безпеки в умовах розбудови інформаційного суспільства, обґрунтовує авторські рекомендації щодо інформаційної складової у забезпеченні національної безпеки держави, а також визначає пріоритетні напрями реалізації державної політики в окресленій сфері.

Метою статті є виявлення особливостей національного інформаційного простору й теоретико-методологічне обґрунтування механізму забезпечення його захисту в умовах України.

Методи дослідження. У роботі використано загальнонаукову методологію проведення наукових досліджень. Так, застосовано методи емпіричних досліджень – спостереження, опису, узагальнення й класифікації (для розгляду предмета дослідження), контент-аналіз (для виокремлення основних характеристик інформаційного простору держави в аспекті його правового регулювання й розгляду в сучасному науковому дискурсі), порівняння (з метою наведення даних щодо місця держави у загальносвітових рейтингах, динаміки державних видатків на досліджувану сферу), а також методи теоретичних досліджень – аналізу і синтезу (з метою розгляду проблеми публічного управління захистом інформаційного простору через її розчленовування на окремі складові елементи й подальше їх об'єднання у цілісну систему), індукції та дедукції (для формулювання висновків і результатів із проведеного дослідження через сходження від загального до конкретного і навпаки).

Виклад основного матеріалу. З огляду на зростання інтересу до питань забезпечення національної безпеки загалом та її складових зокрема важливо розглядати ці поняття у нерозривній єдності, фокусуючи увагу на їх взаємозалежності та взаємовпливах. Відповідно у запропонованій О. Резніковою багаторівневій комплексній моделі забезпечення національної стійкості з-поміж пріоритетних сфер і напрямів на національному, регіональному й місцевому рівнях виокремлено стійкість до інформаційних впливів, де масштабність відповідного ефекту й зв'язок зі станом національної безпеки [1, с. 44, 161] відіграють, на думку авторки, ключову роль.

Така теза закріплена в Україні й на законодавчому рівні. Так, в Указі Президента України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про запровадження національної системи стійкості"» [5] наголошено на тому, що новітня реальність загалом формується

в умовах надзвичайно стрімкого розвитку сучасних технологій, що своєю чергою змінює усталені, традиційні уявлення суспільства про суть загроз будь-якого ґатунку. Суспільна дійсність диктує нові умови зародження, виникнення й розвитку різноманітних надзвичайних та кризових ситуацій, розуміння яких і запровадження ефективних методів подолання яких потребує системного аналізу та оцінювання ризиків у різних сферах життєдіяльності, де одну із провідних ролей відіграють інформаційна й кібернетична (наприклад, захищеність та безперебійне функціонування інформаційно-телекомунікаційних послуг, забезпечення суспільної стійкості до інформаційних впливів і кіберстійкості національних інформаційних ресурсів, навички роботи з дезінформацією тощо).

Велике розмаїття загроз і викликів у інформаційній сфері стало поштовхом до розроблення шляхів їхньої класифікації. Одним із варіантів такого бачення є систематизація загроз у реалізації політики державної безпеки в інформаційній сфері України, запропонована Ю. Правом, а саме:

– загрози у реалізації політики державної безпеки в інформаційній сфері України:

а) загальнодержавні, організаційно-управлінські;

б) політико-правові;

в) фінансово-економічні;

г) інформаційні;

– загрози інформаційній безпеці:

а) політично-інформаційні;

б) інформаційно-економічні;

в) інформаційно-пропагандистські;

г) кіберзагрози [3, с. 80].

Розвиток уявлень про сферу інформаційної безпеки в контексті цивільного захисту пропонує колектив авторів [6], який вважає, що «на сьогодні цивільний захист відіграє полікомпонетну роль у забезпеченні національної безпеки держави», а до функцій єдиної державної системи цивільного захисту в аспекті забезпечення інформаційної безпеки пропонує віднести:

–організацію оповіщення органів влади та населення про

загрозу чи виникнення надзвичайних ситуацій різного характеру;

–інформаційну підтримку (інформування) населення в районах виникнення надзвичайних ситуацій;

–забезпечення захисту інформації (зокрема захисту інформаційних систем) в інтересах державної системи цивільного захисту в різних режимах її функціонування [6, с. 139–140].

Із таким твердженням ми погоджуємося лише частково, адже воно, на наш погляд, не передає всієї повноти завдань, які стоять перед системою публічного управління захистом інформаційного простору як загалом, так і в умовах загрози чи виникнення надзвичайних ситуацій зокрема.

Нам імпонує теза В. Торічного про те, що інформаційна безпека у сфері державно-управлінських відносин має розглядатись як сукупність взаємодіючих і взаємопов'язаних компонентів, зокрема:

–загрози життєво важливим інтересам суспільства у сфері інформаційної безпеки, а також небезпеки, виклики та ризики;

–життєво важливі інтереси суспільства, держави та особистості, що підлягають інформаційному захистові;

–основні заходи, що проводяться суб'єктами механізму держави, представниками громадянського суспільства щодо нейтралізації загроз, небезпек і ризиків у сфері інформаційної безпеки [4, с. 114].

З огляду на це варто зважати на те, що глобальний інформаційний простір формується й розвивається досить стрімко, в інформаційній сфері людства відбуваються революційні зміни і трансформації, які активізують нові глобальні виклики й загрози, що становлять реальну небезпеку для людства та міжнародного правопорядку, а наслідки використання сучасної інформаційної зброї можуть бути зіставними із застосуванням зброї масового ураження [7].

У розвиток означеного В. Копанчук виокремлює такі загрози національній безпеці на рівні інформаційної сфери, властиві нашій державі:

–недосконалість нормативно-правової бази, якою унормовано сферу інформаційної безпеки на галузевому рівні;

–недостатній рівень розвиненості інформаційно-телекомунікаційної інфраструктури національного масштабу;

–непослідовність державної політики щодо забезпечення інформаційної безпеки, побудованої на принципах системності, комплексності й ефективності, перевантажена й неефективна система державного управління й регулювання в означеній сфері;

–відсутність дієвих механізмів реалізації операцій інформаційно-психологічного типу, системи, що забезпечує активний кіберзахист інформаційного простору країни, а також надає асиметричну відповідь агресору;

–інформаційна війна інших держав проти України;

–зосередження засобів масової інформації загальнодержавного рівня в руках окремих груп стейкхолдерів;

–дезінформація громадян України та застосування проти них технологій інформаційно-психологічного маніпулятивного характеру [8, с. 196–197].

За таких складних обставин досягнути оптимального функціонування національного інформаційного простору видається хоча і надважким, однак повністю реальним завданням.

Так, нині в Україні розроблення загальнодержавних документів стратегічного значення, дотичних до сфери забезпечення безпеки держави як в цілому, так і стосовно окремих її компонентів, на наш погляд, має бути зорієнтоване на такі три альтернативи, запропоновані О. Резніковою, а саме:

–зменшення негативних впливів загроз будь-якого характеру або забезпечення швидкого відновлення системи публічного управління після надзвичайних і кризових явищ;

–пріоритетність превентивних або реактивних заходів реагування держави на загрозу;

–пріоритетність заходів щодо забезпечення готовності й прогнозування загроз, ефективний кризовий менеджмент, нарощування безпекових спроможностей [1, с. 113].

Одним із показників ефективності національного законодавства в означеній сфері, що наочно ілюструє прогрес держави, є рейтингування країн за критеріями оцінювання їх спроможностей у відповідній галузі. Провідними й

загальновизнаними рейтингами сфери інформаційної та кібернетичної безпеки є Global Cybersecurity Index [9] та National Cyber Security Index [10], кожен з яких ми розглянемо більш докладно нижче.

Глобальний індекс кібербезпеки (Global Cybersecurity Index – GCI), перша редакція якого була опублікована у 2015 р., спрямований на визначення сфер і напрямів кібербезпеки, що потребують подальшого удосконалення державами, долученими до цієї ініціативи. Таким чином, розробляються практичні рекомендації національного рівня з урахуванням регіональної та галузевої специфіки, які в сукупності впливають на підвищення загальносвітового рівня кібербезпеки, поширення та упровадження передового досвіду, формування глобальної культури кібербезпеки тощо.

Сфера охоплення та структура GCI унормовані Резолюцією 130 [11], що нормативно закріплює посилення ролі й значущості Міжнародного союзу електрозв'язку (ITU) – спеціалізованої агенції ООН щодо ІКТ – з питань зміцнення довіри та забезпечення належного рівня безпеки у застосуванні інформаційно-телекомунікаційних технологій за п'ятьма основними сферами: правовою, технічною, організаційною, розвитком потенціалу, співробітництвом.

За даними GCI 2020 року [9], Україна посіла 78 місце з-поміж 194 країн, залучених до анкетування загалом, та 39 місце із 46 держав, які входять до європейського регіону (див. табл. 1).

Національний індекс кібербезпеки (National Cyber Security Index – NCSI) – це глобальний індекс, який в режимі реального часу вимірює готовність країн запобігати кіберзагрозам та управляти кіберінцидентами. Цей індекс сфокусовано на окремих аспектах кібербезпеки, що запроваджуються урядами на національних рівнях за чотирма сферами – чинного законодавства, сформованих інституцій, форматами співпраці, результатами.

Таблиця 1 - Рейтинг країн за Глобальним індексом кібербезпеки (GCI)

Рейтинг	*Країна*	*Оцінка*	*Рейтинг*	*Країна Європи*	*Оцінка*
1	США	100	1	Сполучене Королівство	99,54
2	Сполучене Королівство	99,54	2	Естонія	99,48
2	Саудівська Аравія	99,54	3	Іспанія	98,52
3	Естонія	99,48	4	Литва	97,93
4	Корея	98,52	5	Франція	97,6
4	Сінгапур	98,52	6	Туреччина	97,5
4	Іспанія	98,52	7	Люксембург	97,41
5	Об'єднані Арабські Емірати	98,06	7	Німеччина	97,41
5	Малайзія	98,06	8	Португалія	97,32
6	Литва	97,93	9	Латвія	97,28
7	Японія	97,82	10	Нідерланди	97,05
8	Канада	97,67	...		
9	Франція	97,6	30	Грузія	81,07
10	Індія	97,5	31	Ісландія	79,81
...			32	Румунія	76,29
70	Узбекистан	71,11	33	Молдова	75,78
71	Йорданія	70,96	34	Словенія	74,93
72	Уганда	69,98	35	Чеська Республіка	74,37
73	Замбія	68,88	36	Монако	72,57
74	Чилі	68,83	37	Болгарія	67,38
75	Кот д'Івуар	67,82	39	Україна	65,93
76	Коста-Ріка	67,45	40	Албанія	64.32
77	Болгарія	67,38	41	Чорногорія	53,23
78	Україна	65,93	42	Ліхтенштейн	35,15

Рейтинг	*Країна*	*Оцінка*
79	Пакистан	64,88
80	Албанія	64,32
…		
180	Екваторіальна Гвінея	1,46
181	КНДР	1,35
182	Мікронезія	0
182	Ватикан	0
182	Ємен	0

Рейтинг	*Країна Європи*	*Оцінка*
43	Боснія і Герцеговина	29,44
44	Андорра	26,38
45	Сан-Марино	13,83
46	Ватикан	0

Джерело: побудовано автором за даними [9]

Так, з метою розроблення оновленої редакції NCSI було загалом вивчено стан кібербезпеки 163 країн світу за показниками ефективності законодавства у сфері кібербезпеки, управління кіберінцидентами, інформаційної безпеки, довірчих послуг, захисту персональних даних, боротьби із кіберзлочинністю тощо. За підсумками дослідження Україна посіла 24 місце зі 163 проаналізованих країн (див. табл. 2).

Таблиця 2 – Рейтинг країн за Національним індексом кібербезпеки (NCSI)

Рейтинг	*Країна*	*Національний індекс кібербезпеки*	*Рівень цифрового розвитку*	*Різниця*
1.	Греція	96,10	64,02	32,08
2.	Бельгія	94,81	74,07	20,74
3.	Литва	93,51	67,34	26,17
4.	Естонія	93,51	75,59	17,92
5.	Чеська Республіка	92,21	69,21	23,00
6.	Німеччина	90,91	80,01	10,90
7.	Румунія	89,61	59,84	29,77
8.	Португалія	89,61	68,46	21,15

Рейтинг	*Країна*	*Національний індекс кібербезпеки*	*Рівень цифрового розвитку*	*Різниця*
9.	Іспанія	88,31	72,21	16,10
10.	Польща	87,01	65,03	21,98
		…		
20.	Малайзія	79,22	62,19	17,03
21.	Італія	79,22	67,26	11,96
22.	Сполучене Королівство	77,92	79,96	-2,04
23.	Швейцарія	76,62	82,93	-6,31
24.	Україна	75,32	55,96	19,36
25.	Латвія	75,32	66,23	9,09
		…		
160.	Домініка	3,90	56,90	-53,00
161.	Соломонові острови	2,60	21,10	-18,50
162.	Тувалу	2,60		
163.	Південний Судан	1,30		

Джерело: побудовано автором за даними [10]

Окрім того, у контексті викладеного вважаємо за необхідне навести дані про видатки Державного бюджету України 2022 р. на сферу захисту інформаційного простору (див. табл. 3), основний фокус якого було спрямовано на підтримання економіки нашої держави в умовах надзвичайних і кризових явищ.

Таблиця 3 – Видатки Державного бюджету України 2022 р. на сферу захисту інформаційного простору

№ з/п	*Показник*	*Сума (грн)*
1	Інформаційно-аналітичне забезпечення координаційної діяльності у сфері національної безпеки і оборони	335126,3
2	Інформаційно-аналітичне забезпечення	53006,2

	діяльності у сфері інформаційної безпеки України	
3	Модернізація цифрових інформаційно-аналітичних систем	50000
4	Електронне урядування	651524
5	Розвиток пріоритетних проектів в галузі інформаційних технологій	450000
6	Національна програма інформатизації	2205274,6
7	Збирання, обробка та розповсюдження офіційної інформаційної продукції	268543,9
8	Здійснення заходів у сфері захисту національного інформаційного простору	50000
Усього:		4 063 475

Джерело: побудовано автором за даними [12]

Примітним є той факт, що показник «здійснення заходів у сфері захисту національного інформаційного простору» для Міністерства культури та інформаційної політики України в розрізі видатків Державного бюджету України з'явився лише у 2018 році, а за результатами аналізу їх розподілу впродовж п'ятирічного періоду встановлено, що він тяжіє до скорочення (див. рис. 1).

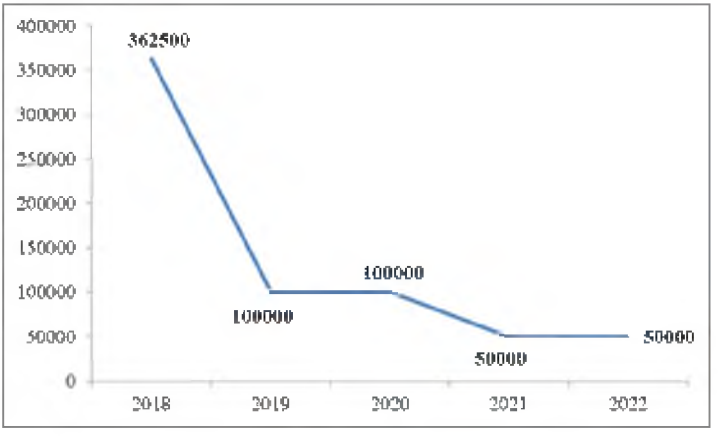

Рис. 1 – Динаміка видатків Державного бюджету України на здійснення заходів у сфері захисту національного інформаційного простору (2018–2022 рр., грн)

Джерело: розроблено автором

Однак інші показники, які є дотичними до сфери захисту інформаційного простору держави й відповідного організаційно-функціонального забезпечення публічного управління, що загалом сприяють зміцненню національної стійкості (див. табл. 3), залишаються сталими із певним збільшенням видатків на сферу національної безпеки і оборони.

Науковці [3, с. 197–199] стверджують, що задля імплементації будь-яких стратегічних планів та відповідних заходів з питань забезпечення безпеки в інформаційній сфері вкрай важливим є налагодження тісної співпраці та взаємодії між державою та суспільством. Такий формат здатний мати значні позитивні ефекти, а саме: для суспільства загалом – його активізація в аспекті забезпечення власної безпеки, підвищення рівня кібербезпеки, розвиток інститутів громадянського суспільства; для окремих індивідів – навички протидії інформаційним загрозам, медіаграмотність, цифрова компетентність; для приватного сектора – підвищення спроможностей у подоланні інформаційних загроз, корпоративної безпеки, налагодження ефективної комунікації; для інститутів громадянського суспільства – інструментарій долучення до процесів і процедур формування й реалізації державної політики у безпековій сфері, громадські ініціативи щодо впровадження інноваційних підходів у відповідну сферу державної політики; для органів публічної влади – одержання додаткових експертних консультацій, вивчення досвіду громадського сектора і міжнародних організацій, залучення інститутів громадянського суспільства безпосередньо до реалізації державної політики, моніторингу та аналізу її ефективності тощо.

Ми погоджуємося із пропозицією про те, що основоположними факторами формування державної системи інформаційної безпеки мають стати законність, чітке розмежування повноважень, добровільність залучення стейкхолдерів, колегіальність управління системою, стабільність ядра системи, адаптивність до змін і умов функціонування, раціональне поєднання універсальності та диференціації механізмів забезпечення інформаційної безпеки, поетапність упровадження [4, с. 246–247] та забезпечення

сталості як цієї підсистеми, так і всієї системи забезпечення національної безпеки держави, адже новітня дійсність значною мірою актуалізує потребу і нагальність відповідної державної політики.

Висновки та перспективи. Проведене дослідження дає змогу зробити певні узагальнення та систематизувати основні підходи щодо забезпечення захисту інформаційного простору держави в умовах України. Так, пріоритетними, на наш погляд, є:

–забезпечення спроможностей держави у секторі безпеки та оборони, зокрема щодо нейтралізації негативних інформаційних впливів, дестабілізуючих і деструктивних явищ, відповідної рішучої протидії;

–посилення здатності суб'єктів механізму держави до реалізації проактивного підходу, зокрема в аспекті імплементації превентивних заходів щодо безпосередніх, опосередкованих, ймовірнісних загроз і відповідного на них реагування;

–проведення інформаційно-роз'яснювальної роботи серед різноманітних суспільних груп та окремих індивідів, представників суб'єктів механізму держави з питань надзвичайних та кризових ситуацій в контексті потенційних ризиків і загроз для національної безпеки держави загалом та її окремих компонентів.

Окреслене коло питань вбачається перспективним для проведення подальших досліджень за означеним напрямом державної політики України.

Список використаних джерел

1. Резнікова О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 456 с.
2. Кантур О. Досвід іноземних держав у питанні протидії інформаційним впливам Російської Федерації. *Вісник КНУ ім. Т. Шевченка. Державне управління.* 2022. Вип. 2(16). С. 5–12.
3. Прав Р. Ю. Механізми формування і реалізації політики державної безпеки в інформаційній сфері : дис. … канд. держ. упр. : спец. 25.00.05 «Держ. упр. у сфері держ. безпеки та охорони гром. порядку» / МАУП. Київ, 2020. 263 с.
4. Торічний В. О. Інформаційне забезпечення безпеки держави в умовах інформаційного суспільства : державно-управлінський аспект : монографія. Харків : НУЦЗУ, 2020. 274 с.
5. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021

року «Про запровадження національної системи стійкості» : Указ Президента України від 27.09.2001 р. № 479/2021. *Офіційний вісник України.* 2021. 79. 31.
6. Цивільний захист у забезпеченні національної безпеки України (основи становлення, сучасний стан, напрямки розвитку) : монографія / О. Я. Лещенко, В. М. Михайлов, М. В. Андрієнко та ін. Київ : ІДУ НД ЦЗ, 2021. 348 с.
7. Пилипчук В. Г. Розвиток правової науки в інформаційній сфері : системні проблеми та пріоритети. *Право України*. 2013. № 9. С. 146–161.
8. Копанчук В. О. Державна політика у сфері національної безпеки та охорони громадського порядку : дис. … докт. держ. упр. : спец. 25.00.05. «Держ. упр. у сфері держ. безпеки та охорони гром. порядку» / НУЦЗУ. Харків, 2020. 375 с.
9. Global Cybersecurity Index 2020. *ITU Publications* : websit. URL : https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (дата звернення : 19.02.2023).
10. National Cyber Security Index. URL : https://ncsi.ega.ee/ (дата звернення : 19.02.2023).
11. Strengthening the role of ITU in building confidence and security in the use of information and communication technologies : Resolution 130 Rev. Dubai, 2018. URL : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/RES_130_rev_Dubai.pdf (дата звернення : 19.02.2023).
12. Про Державний бюджет України на 2022 рік : Закон України від 02.12.2021 р. № 1928-IX. *Офіційний веб-портал парламенту України.* URL : https://zakon.rada.gov.ua/laws/show/1928-20#Text (дата звернення : 20.02.2023).

References

1. Reznikova, O. (2022). *Natsionalna stiikist v umovakh minlyvoho bezpekovoho seredovyshcha* [National resilience under conditions of a changing security environment]. Kyiv: NISD [in Ukrainian].
2. Kantur, O. (2022). Dosvid inozemnykh derzhav u pytanni protydii informatsiinym vplyvam Rosiiskoi Fereratsii [Experience of foreign states in the issue of counterfeiting information influences of the Russian Federation]. *Visnyk KNU im. T. Shevchenka. Derzhavne upravlinnia,* 2 (16), 5–12. [in Ukrainian].
3. Prav, R. Yu. (2020). *Mekhanizmy formuvannia i realizatsii polityky derzhavnoi bezpeky v informatsiinii sferi* [Mechanisms of formation and implementation of state security policy in the information sphere]. (Candidates thethis). MAUP. Kyiv [in Ukrainian].
4. Torichnyi, V. O. (2020). Informatsiine zabezpechennia bezpeky derzhavy v umovakh informatsiinoho suspilstva: derzhavno-upravlinskyi aspekt [Information provision of state security under conditions of the information society: public-administrative aspect]. Kharkiv: NUTsZU [in Ukrainian].
5. On the decision of the National Security and Defense Council of Ukraine dated August 20, 2021 «On the introduction of the national stability system»: Decree of the President of Ukraine from September 27, 2001. № 479/2021. (2021). *Ofitsiinyi visnyk Ukrainy,* 79, 31. [in Ukrainian].
6. Leshchenko, O. Ya., Mykhailov, V. M., Andriienko, M. V. et al. (2021). Tsyvilnyi zakhyst u zabezpechenni natsionalnoi bezpeky Ukrainy (osnovy stanovlennia, suchasnyi stan, napriamky rozvytku) [Civil protection in ensuring the national security of Ukraine (fundamentals of formation, current state, development prospects)]. Kyiv: IDU ND TsZ [in Ukrainian].
7. Pylypchuk, V. H. (2013). Rozvytok pravovoi nauky v informatsiinii sferi: systemni problemy ta priorytety [Development of legal science in the information field: systemic problems and priorities]. *Pravo Ukrainy*, 9, 146–161 [in Ukrainian].

8. Kopanchuk, V. O. (2020). Derzhavna polityka u sferi natsionalnoi bezpeky ta okhorony hromadskoho poriadku [State policy in the field of national security and protection of public order] (Doctors thesis). NUTsZU. Kharkiv [in Ukrainian].
9. Global Cybersecurity Index 2020. *TU Publications*: websit. Retrieved from https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E [in English].
10. National Cyber Security Index. Retrieved from https://ncsi.ega.ee/ [in English].
11. Strengthening the role of ITU in building confidence and security in the use of information and communication technologies: Resolution 130. (2018). Rev. Dubai. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents /RES_130_rev_Dubai.pdf. [in English].
12. Law of Ukraine On the State Budget of Ukraine for 2022 from December 2, 2021 № 1928-IX. *Ofitsiinyi veb-portal parlamentu Ukrainy*. Retrieved from https://zakon.rada.gov.ua/laws/show/1928-20#Text [in Ukrainian].

INFORMATION SPACE OF THE STATE AND PROBLEMS OF ENSURING ITS PROTECTION IN UKRAINE

Hlobenko Serhii

Abstract. Taking into account an inconstant and rapidly changing environment, the main approaches of the state in ensuring effective construction and stable functioning of its information space are characterized, which in current conditions acquires a particularly important, conceptual meaning. The problems of state policy in the information sphere are studied with an emphasis on guaranteeing information security, a significant interest in which is dictated by the modern social reality. Views on ensuring national security and defense of the state in the face of the latest threats and challenges in terms of the need to achieve the maximum possible stability of both its certain components and the system as a whole are considered, which is caused by the complex conditions of its current functioning and the need for its further preservation. The features of the national information space are singled out and the main problems of its further development are clarified, taking into account ensuring security of an individual, society, and the state as one of the fundamental factors of the state mechanism's functioning, characterized by a significant level of complexity and being multifaceted, which currently under Ukrainian conditions requires the search for the most effective administrative decisions. The role and place of Ukraine in global ratings of security capabilities in the field of protection of information space, the relevant mechanisms of public administration, as well as the main causes that influence these processes are analyzed. The factors of the formation of the state information security system, directions of implementation of strategic plans and relevant measures for ensuring security in the information sphere under conditions of emergencies and crises are summarized and systematized, theoretical and applied aspects of prospects for the further development of information space of the state and ensuring its protection in Ukrainian conditions are described.

Key words: information space of the state, information security, protection of information space, state policy in the information sphere, mechanisms of public administration.