УДК 352[329.09.5]:355.01
DOI https://doi.org/10.51547/ppp.dp.ua/2025.2.18

Ворчило Владислав Олегович,
здобувач ступеня доктора філософії,
Національного університету «Чернігівська політехніка»
ORCID ID: 0009-0007-9927-1570

МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕРИТОРІАЛЬНИХ ГРОМАД: ПРОБЛЕМИ РЕАЛІЗАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

MECHANISMS OF STATE ADMINISTRATION IN THE SPHERE OF INFORMATION SECURITY OF TERRITORIAL COMMUNITIES: PROBLEMS OF IMPLEMENTATION IN CONDITIONS OF MARTIAL STATE

У статті розглянуто питання визначення шляхів вирішення проблем вироблення та реалізації механізмів державного управління у сфері інформаційної безпеки на рівні територіальних громад в умовах дії правового режиму воєнного стану. Увагу приділено пріоритетності реалізації інформаційної політики та важливість функціонально-цільової орієнтації механізмів державного управління у сфері інформаційної безпеки, перш за все, на регіональному рівні, тобто рівні територіальних громад, які є не тільки базовими суб'єктами реалізації інформаційної політики, але й, враховуючи сучасну ситуації в державі, пов'язану з повномасштабною війною, залишаються одним з основних об'єктів інформаційного впливу з боку противника, що загострює проблеми забезпечення інформаційної безпеки та вироблення адекватних механізмів державного управління у цій сфері. Акцентовано увагу на тому, що сфери застосування цифрових технологій в управлінні територіальними громадами є потенційними об'єктами впливу з боку противника й, за умов відсутності або ненадійності заходів щодо забезпечення інформаційної безпеки, здатні зруйнувати сталі зв'язки та привести до дезорганізації не тільки управління на рівні державної та місцевої влади, але й дезорганізації соціально-економічного життя регіонів, основою чого залишаються в сучасних умова державотворення територіальні громади. З урахуванням наведених концептуальних положень, стратегічних цілей, визначених стратегією інформаційної безпеки держави, а також основних напрямів реалізації державної інформаційної політики, спрямованих на вирішення наявних проблем у цій сфері, в умовах дії правового режиму воєнного стану визначено основні механізми державного управління у сфері інформаційної безпеки територіальних громад.

Ключові слова: *державне управління, інформаційна безпека, механізми державного управління, національна безпека, правовий режим воєнного стану, територіальні громади.*

The article considers the issue of determining ways to solve the problems of developing and implementing mechanisms of state governance in the field of information security at the level of territorial communities under the legal regime of martial law. Attention is paid to the priority of implementing information policy and the importance of the functional and target orientation of mechanisms of state governance in the field of information security, primarily at the regional level, that is, the level of territorial communities, which are not only the basic subjects of implementing information policy, but also, taking into account the current situation in the state, associated with a full-scale war, remain one of the main objects of information influence from the enemy, which exacerbates the problems of ensuring information security and developing adequate mechanisms of state governance in this area. Attention is drawn to the fact that the areas of application of digital technologies in the management of territorial communities are potential objects of influence from the enemy and, in the absence or unreliability of measures to ensure information security, are capable of destroying stable connections and leading to the disorganization of not only management at the level of state and local authorities, but also the disorganization of the socio-economic life of regions, the basis of which remains territorial communities in modern conditions of state formation. Taking into account the above conceptual provisions, strategic goals defined by the state's information security strategy, as well as the main directions of the implementation of state information policy aimed at solving existing problems in this area, under the conditions of the legal regime of martial law, the main mechanisms of state management in the field of information security of territorial communities have been determined.

Key words: *public administration, information security, public administration mechanisms, national security, legal regime of martial law, territorial communities.*

Постановка проблеми. Введення в дію правового режиму воєнного стану як відповідь на збройну агресію з боку РФ проти України потребувало зміни принципів та підходів до державного управління у різних сферах життєдіяльності суспільства і держави. Прагнення держави протисто-

яти наявним та потенційним загроз національній безпеці на практиці орієнтується на вироблення нових адекватних ситуації механізмів державного управління, які розглядаються в якості основи вирішення наявних проблем, та стосуються всіх рівнів організації суспільного життя та реалізації публічної влади в Україні. Водночас з активізацією бойових дій на території України, противник суттєво посилив інформаційно-психологічний вплив на населення регіонів держави, що потенційно і реально несе в собі загрозу національній безпеці. У цьому контексті вироблення та реалізація механізмів державного управління у сфері інформаційної безпеки привертає особливу увагу, зокрема ураховуючи наявність тимчасово окупованих територій, територій держави, наближених до ведення активних бойових дій тощо, що потребує визначення шляхів вирішення проблем вироблення та реалізації механізмів державного управління у сфері інформаційної безпеки на рівні територіальних громад в умовах дії правового режиму воєнного стану.

Аналіз останніх досліджень та публікацій. Вітчизняними науковцями було розглянуто низку питань, пов'язаних з визначення передумов вироблення та реалізації механізмів державного управління у сфері інформаційної безпеки, у тому числі на рівні територіальних громад. Ці питання розглядали Ю. Богач [1], А. Геворкян [3], С. Горбаченко [4], С Квітка [5], Н. Литвин [7], С. Свєшніков [14], А. Соколов [4], В. Шемчук [11] та інші дослідники. Проблеми забезпечення національної безпеки в умовах інформаційно-психологічного впливу на суспільство, державу і особистість розглядали Д. Вітер [2], Л. Мазуренко [8], Ю. Ніколаець [9], О. Руденко [2] та інші дослідники. Поряд з цим дослідження, що стосуються проблем і перспектив вироблення формування механізмів державного управління у сфері інформаційної безпеки на рівні територіальних громад, у тому числі в умовах дії правового режиму воєнного стану, залишається малодослідженим.

Метою статті є визначення шляхів вирішення проблем вироблення та реалізації механізмів державного управління у сфері інформаційної безпеки на рівні територіальних громад в умовах дії правового режиму воєнного стану.

Виклад основного матеріалу. У літературі пропонується розуміти «механізм забезпечення інформаційної безпеки як регламентовану законодавством діяльність уповноважених суб'єктів, спрямовану на охорону та захист інформаційної сфери особи, суспільства та держави від зовнішніх і внутрішніх загроз й удосконалення заходів інформаційної протидії та боротьби» [11, с. 56]. Таке розуміння в цілому дає можливість вказати на наступні механізми державного управління у сфері інформаційної безпеки: інформаційний патронат, інформаційний захист, інформаційну кооперацію, формування ефективних систем захисту інформації, які спрямовуються на конкретні сфери життєдіяльності суспільства, держави і особистості, функціонуючи у просторі інформаційної політики держави, що визначає завдання того чи іншого механізму державного управління у сфері забезпечення інформаційної безпеки (Див. рис. 1).

Зважаючи на такий підхід до формування та реалізації механізмів державного управління у сфері інформаційної безпеки, ми має акцентувати увагу на тому, що «за рівнями соціальної організації та геополітичним змістом інформаційна безпека повинна забезпечуватися на міждержавному, загальнодержавному та внутрішньодержавному рівнях (на рівні регіональних інститутів), а також на рівні органів місцевого самоврядування. Тобто, головними суб'єктами інформаційної безпеки виступає як держава, що здійснює свої функції через відповідні органи, так і громадяни, суспільні або інші організації чи об'єднання, що володіють повноваженнями із забезпечення інформаційної безпеки відповідно до законодавства» [1, с. 25]. Відтак, фактично стверджується пріоритетність реалізації інформаційної політики та важливість функціонально-цільової орієнтації механізмів державного управління у сфері інформаційної безпеки, перш за все, на регіональному рівні, тобто рівні територіальних громад, які є не тільки базовими суб'єктами реалізації інформаційної політики, але й, ураховуючи сучасну ситуації в державі, пов'язану з повномасштабною війною, залишаються одним з основних об'єктів інформаційного впливу з боку противника. Це загострює проблеми забезпечення інформаційної безпеки та вироблення адекватних механізмів державного управління у цій сфері.

Так, проблема використання інформаційно-комунікаційних технологій та відповідних механізмів державного управління у сфері національної безпеки, пов'язана з тим, що, з одного боку, дійсно, «інформаційно-комунікаційні технології соціально-економічного розвитку суттєво поліпшують інформаційне забезпечення усіх зацікавлених сторін, забезпечують відкритість управління, підвищують сту-пінь обґрунтованості прийнятих рішень та сприяють кращому усвідомленню цілей розвитку громади» [4, с. 170], але з іншого – ці технології в умовах ведення державою повно-

масштабної війни перетворюються на загрози, які мають не тільки характер локальної, але й регіональної загрози державній безпеці. Крім цього, особливості сучасних процесів державотворення, які підпадають активному впливу тих чи інших феноменів інформаційного суспільства, стрімкого розвитку інформаційних технологій, зокрема дітжиталізації (цифровізації) [5; 7], обумовлюють необхідність на всіх рівнях державного будівництва здійснювати постійне удосконалення наявних та вироблення нових механізмів державного управління у сфері інформаційної безпеки. У цьому контексті, ураховуючи децентралізацію влади в державі, отримання місцевою владою значного обсягу повноважень у прийнятті та реалізації рішень, що стосуються розвитку територіальних громад, питання забезпечення їх інформаційної безпеки набуває пріоритетності, адже «територіальні громади, особливо у великих містах, можуть стати об'єктом кібератак, спря-мованих на викрадення чутливої інформації, параліза-цію муніципальних служб або навіть шантажу» [4, 170], а в умовах ведення активних бойових дій – об'єктом впливу противника, який постійно нарощує спроможності щодо проведення інформаційно-психологічних операцій. Тому питання вироблення механізмів державного управління у сфері інформаційної безпеки територіальних громад на сучасному етапі розвитку суспільства і держави виявляється вкрай актуальним, адже дійсно, «інформаційна діяльність є важливою компонентою інформаційної безпеки

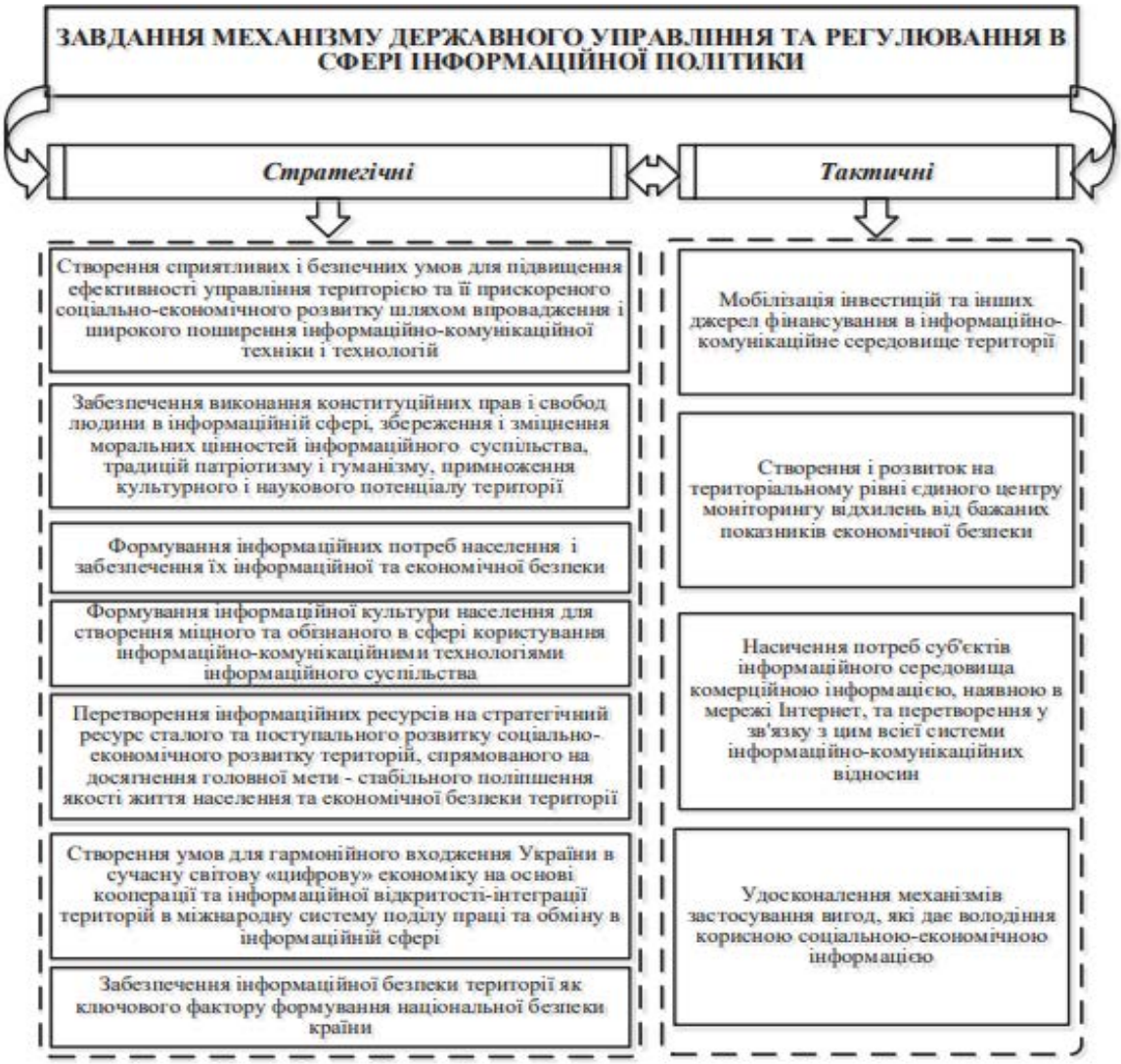

Рис. 1. Стратегічні та тактичні завдання механізму державного управління та регулювання у сфері інформаційної політики

Джерело: [3, с. 102].

і невід'ємною складовою частиною виживання громадян та їх територіальних об'єднань. Тому, до головних стратегічних цілей інформаційної діяльності органів місцевого самоврядування окрім створення умов для підвищення ефективності управління місцевою територіальною громадою необхідно віднести забезпечення інформаційної безпеки» [1, с. 26-27].

У цьому аспекті, якщо звернути увагу на сфери застосування цифрових технологій в управлінні територіальними громадами (Див. рис. 2), можна побачити, що всі наявні напрямки є потенційними об'єктами впливу з боку противника й, за умов відсутності або ненадійності заходів щодо забезпечення інформаційної безпеки, здатні зруйнувати сталі зв'язки та привести до дезорганізації не тільки управління на рівні державної та місцевої влади, але й дезорганізації соціально-економічного життя регіонів, основою чого залишаються в сучасних умова державотворення територіальні громади.

Водночас, варто підкреслити, що основні сфери застосування механізмів державного управління із забезпечення інформаційної безпеки на рівні територіальних громад не мають обмежуватись захистом особистих даних громадян, функціонуванням публічних служб, впровадженням електронного врядування, ефективних функціонуванням інфраструктури, економічною безпекою та захисту від кіберзлочинності та кібертероризму, як вважає більшість дослідників [4; 7], які обґрунтовують свою позицію тим, що «територіальні громади здійснюють різноманітні адміністративні та соціальні функції, велика частина яких базується на обміні та зберіганні інформації, тому вразливість системи може призвести до порушення роботи та непередбачених наслідків для громадян» [4, с. 174]. Така ситуація загострюється й тим, що «інтернет, як основа інформаційних систем командування, контролю, каналів зв'язку, комп'ютерів, спостереження та розвідки, що забезпечує створення певного єдиного інформаційного простору на полі бою, залишається одним з головних елементів інформаційно-комунікативної системи управління не лише різними засобами ведення війни, але й ведення боротьби нового покоління» [2, с. 120] – ведення війни в інформаційному просторі. Як підкреслюють дослідники, «щоб зменшити втрати ЗС та збільшити потік інформації про порушення ворогом умов ведення війни через інформаційно-комунікативну систему проводиться компанія «віктимізації за довіреністю» (формування макровіктимного мислення) шляхом поширенням фейків і посиленою пропагандистською кампанією всередині країн ЄС та США, спрямованою на протидію РФ. У даному випадку вибірковість у підборі інформації та атаках на свідомість людей – обов'язковий механізм віктимізації» [2, с. 120].

Зрозуміло, що «під час війни, надзвичайно важливим стає нейтралізація численних інфор-

Рис. 2. Напрямки обміну інформацією на рівні ТГ

Джерело: [4, с. 171]

маційних загроз, для чого необхідно проведення низки організаційно-правових заходів», а саме [8, с. 55]:

– стратегічне стримування та припинення бойових дій та військових конфліктів, що можуть виникнути після зумисного застосування дезінформаційних технологій;

– поліпшення системи забезпечення інформаційної безпеки ЗСУ, інших військових формувань, включно з силами та засобами інформаційної протидії;

– прогнозування, виявлення та оцінка загроз, включаючи загрози для ЗСУ в сфері інформації.

Інакше кажучи, йдеться про основу вироблення та реалізації механізмів державного управління у сфері інформаційної безпеки на рівні територіальних громад, оскільки саме цей рівень безпосередньо пов'язаний у тому числі й з проблемами забезпечення інформаційної безпеки ЗС України, чому сприяє (як виникнення загроз, так і можливості їх мінімізації) локалізація підрозділів ЗС на конкретних територіях держави, що репрезентовані конкретними територіальними громадами. Зважаючи на це та ураховуючи наявність складних комплексних проблем, тенденція, що розвивається наразі у сфері забезпечення інформаційної безпеки, передбачає, що забезпечення протидії комплексу загроз інформаційній безпеці України, потребує [6]:

1. Виваженої державної політики у сфері інформаційної безпеки, яка враховує зовнішні і внутрішні загрози національній безпеці в інформаційній сфері, перш за все, загрози комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації, а також загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору. До загрози комунікативного характеру включають:

а) зовнішні негативні інформаційні впливи на свідомість людини та спільноти через засоби масової інформації, а також мережу Інтернет з метоюзміни психічного та емоційного стану людини, її психологічних і фізіологічних характеристик; здійснення керованого впливу на свободу вибору; поширення закликів до сепаратизму, повалення конституційного ладу чи порушення територіальної цілісності держави;

б) інформаційний вплив на населення України, у тому числі на особовий склад військових формувань, мобілізаційний резерв, з метою послаблення їх готовності до оборони держави;

в) поширення суб'єктами інформаційної діяльності інформації, яка дискредитує органи державної влади, дестабілізує суспільно-політичну ситуацію тощо.

До загрози технологічного характеру у сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору, включають:

а) використання іноземними державами кібервійськ, кіберпідрозділів, нових видів інформаційної зброї та зброї кібернетичного характеру на шкоду Україні;

б) прояви кіберзлочинності, кібертероризму чи кібернетичної військової агресії, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем, шляхом втручання, несанкціонованого доступу або порушення функціонування телекомунікаційних, кібернетичних, автоматизованих комп'ютерних систем, незалежно від форми власності, з метою: вчинення диверсій чи терористичних актів; здійснення підтримки, супроводження чи активізації злочинної, екстремістської чи терористичної діяльності; здійснення з їх допомогою деструктивного інформаційного впливу; перехоплення інформації в телекомунікаційних мережах; створення радіоелектронних перешкод чи блокування інформаційних систем, засобів зв'язку та управління, реалізація програмно-математичних засобів, що порушують функціонування інформаційних систем; включення у програмно-технічні засоби прихованих шкідливих функцій тощо.

З урахуванням наведених концептуальних положень, стратегічних цілей, визначених стратегією інформаційної безпеки держави [10], а також основних напрямів реалізації державної інформаційної політики [9], спрямованих на вирішення наявних проблем у цій сфері, в умовах дії правового режиму воєнного стану серед основних механізмів державного управління у сфері інформаційної безпеки територіальних громад необхідно головну увагу звернути на вироблення та імплементацію у практику наступних механізмів:

– створення та розвиток системи мовлення територіальних громад;

– розширення комунікативних можливостей та зниження конфліктності всередині територіальних громад;

– підвищення рівня інформаційного забезпечення територіальних громад;

– контроль впливу онлайн-контенту нових засобів масової інформації на суспільну думку представників територіальних громад;

– розширення співпраці органів місцевого самоврядування з інститутами громадянського суспільства з питань протидії дезінформації;

– моніторинг інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави на локальному рівні;

– підготовка та проведення інформаційних заходів, координацію залучення до них представників територіальних громад;

– включення територіальних громад до процесу розвитку та функціонування системи стратегічних комунікацій;

– здійснення правових, організаційних, технічних, інформаційних та інших дій щодо забезпечення інформаційної безпеки на рівні територіальних громад (зокрема в місцях дислокації, розгортання та застосування угруповань, військових частин та підрозділів Збройних Сил України, інших військових формувань, утворених відповідно до законів України);

– підготовка до протидії інформаційним операціям та іншим заходам інформаційного впливу противника на рівні територіальних громад.

Висновки. Таким чином, вироблення та реалізація механізмів державного управління у сфері інформаційної безпеки привертає особливу увагу, зокрема ураховуючи наявність тимчасово окупованих територій, територій держави, наближених до ведення активних бойових дій тощо, що обумовлює визначення шляхів вирішення проблем вироблення та реалізації механізмів державного управління у сфері інформаційної безпеки на рівні територіальних громад в умовах дії правового режиму воєнного стану. Найбільш визначними з огляду на ситуацію в державі у комплексі таких механізмів є розширення комунікативних можливостей та зниження конфліктності всередині територіальних громад; контроль впливу онлайн-контенту нових засобів масової інформації на суспільну думку представників територіальних громад; розширення співпраці органів місцевого самоврядування з інститутами громадянського суспільства з питань протидії дезінформації; моніторинг інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави на локальному рівні; підготовка та проведення інформаційних заходів, координацію залучення до них представників територіальних громад тощо.

REFERENCES:

1. Bohach Yu. Informatsiina bezpeka yak nevidiemna skladova vidnovlennia ta rozvytku terytorialnykh hromad. IV Vseukrainska naukovo-praktychnakonferentsiia z mizhnarodnoiu uchastiu. S. 25-27.

2. Viter D., Rudenko O. Informatsiino-komunikatyvna skladova merezhevoi protydii zahrozam natsionalnii bezpetsi u voiennii sferi. Society and Security. 2024. № 1(2). S. 119-123. DOI: https://doi.org/10.26642/sas-2024-1(2)-119-123.

3. Hevorkian A. Mekhanizmy derzhavnoho upravlinnia ta rehuliuvannia u sferi informatsiinoi polityky yak faktor zmitsnennia ekonomichnoi bezpeky terytorii. Pravo ta derzhavne upravlinnia. 2021. № 2. S. 98-105. DOI https://doi.org/10.32840/pdu.2021.2.15.

4. Horbachenko S., Sokolov A., Klievtsievych N. Rol informatsiino-komunikatsiinykh tekhnolohii v zabezpechenni zakhystu informatsii na rivni terytorialnykh hromad. Ekonomichnyi visnyk NTUU «Kyivskyi politekhnichnyi instytut». 2024. № 29. S. 169-176.

5. Kvitka S., Novichenko N., Husarevych N., Piskokha N., Bardakh O. Demoshenko H. Perspektyvni napriamky tsyfrovoi transformatsii publichnoho upravlinnia. Aspekty publichnoho upravlinnia. 2020. № 8(4). S. 129-146.

6. Kontseptsiia informatsiinoi bezpeky Ukrainy (proekt). – URL: https://www.osce.org/files/f/documents/0/2/175056.pdf.

7. Lytvyn N., Krupnova L. Didzhytalizatsiia yak zasib pidvyshchennia vidkrytosti, prozorosti ta efektyvnosti diialnosti orhaniv derzhavnoi vlady ta orhaniv mistsevoho samovriaduvannia shchodo nadannia elektronnykh posluh. Irpinskyi yurydychnyi chasopys: naukovyi zhurnal. 2020. №. (2). S. 69-75.

8. Mazurenko L. Informatsiina bezpeka v umovakh Rosiisko-Ukrainskoi viiny: vyklyky ta zahrozy. Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina, seriia «Pytannia politolohii». 2022. Vyp. 42. S. 50-57. https://doi.org/10.26565/2220-8089-2022-42-08.

9. Nikolaiets Yu. Derzhavna informatsiina polityka Ukrainy v umovakh povnomasshtabnoho voiennoho vtorhnennia Rosiiskoi Federatsii: suspilno-mobilizatsiinyi potentsial i efektyvnist. Politychni doslidzhennia. 2024. № 1 (7). S. 42-67. DOI: https://doi.org/10.53317/2786-4774-2024-1-3.

10. Ukaz Prezydenta Ukrainy №685/2021 «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky». – URL: https://www.president.gov.ua/documents/6852021-41069/

11. Shemchuk V. Mekhanizm zabezpechennia informatsiinoi bezpeky derzhavy: teoretychno-metodolohichni osnovy. Filosofski ta metodolohichni problemy prava. 2019. № 1 (17). S. 51-59. DOI: https://doi.org/10.33270/01191702.51.