УДК 004.056.5:351.861(477) **DOI:** https://doi.org/10.32631/v.2024.1.24

Олексій Юрійович Старостін,
Національний юридичний університет імені Ярослава Мудрого,
Інститут підготовки юридичних кадрів для Служби безпеки України,
спеціальна кафедра № 4 (старший викладач);
https://orcid.org/0009-0009-4329-6247,
e-mail: starostinolexi37@gmail.com

ОСНОВНІ ЗАГРОЗИ ІНТЕРЕСАМ ДЕРЖАВИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

У статті наголошено на тому, що в умовах значного впливу інформації на життя суспільства одними з основних загроз, які постають перед сучасними державами, виступають саме інформаційні. У сфері інформаційної безпеки України виокремлено такі загрози: використання інформаційного впливу задля спотворення думки населення щодо політичної ситуації; недосконале нормативно-правове забезпечення інформаційної безпеки держави; навмисне викривлення інформації на рівні лідерів держав і дипломатичних представників; недостатня участь населення України у протидії інформаційним атакам; недосконаліть інституційного й організаційного забезпечення освіти з інформаційної безпеки та формування культури інформаційної безпеки в суспільстві.

Ключові слова: інформаційна безпека, інтереси держави, основні загрози, інформаційна війна.

Оригінальна стаття

Постановка проблеми

Захист інтересів держави є невід'ємною частиною діяльності органів державної влади, їх посадових осіб та органів місцевого самоврядування [1, p. 65]. Водночас інтереси держави на сучасному етапі розвитку людства поступово все більше переходять в інформаційну сферу, адже однією з найважливіших характеристик сучасного етапу розвитку цивілізації є масова інформатизація всіх сторін життя. Інформація є базовою складовою будь-якого сучасного суспільства, яку ще називають «інформаційною» [2, p. 284], а закріплення права на інформацію є невід'ємною частиною європейської правової традиції його розуміння як інструменту комунікативної взаємодії особи та держави в процесі прийняття публічних рішень [3, p. 158].

В умовах такого значного впливу інформації на життя суспільства одними з основних загроз, які постають перед сучасними державами, виступають саме інформаційні. З огляду на це в наш час мають місце повномасштабні інформаційні війни, спрямовані на всебічне

перешкоджання нормальному функціонуванню держави в інформаційній сфері, зокрема з початком російсько-української війни значна увага держави-агресора прикута саме до інформаційної сфери як однієї з базових сфер життєдіяльності українського суспільства.

Стан дослідження проблеми

В українській правовій доктрині окремим проблемам інформаційної безпеки держави присвячували дослідження такі провідні вітчизняні науковці, як-от: І. Арістова, Ю. Безуса, О. Брусакова, В. Важинський, А. Єфремов, О. Журавель, І. Зозуля, О. Зозуля, Т. Кагановська, О. Капля, Д. Кошиков, Т. Кузубова, Ю. Курилюк, А. Лубенцов, О. Манжай, О. Музичук, І. Мірошников, В. Невядовський, І. Панова, І. Пахомова, Д. Сімонович, Д. Тихонова, О. Шайтуро та ін. Окремі проблемні аспекти освіти у сфері інформаційної безпеки, формування культури інформаційної безпеки та інші актуальні питання за темою дослідження розглядали такі зарубіжні дослідники, як М. Алнатір, А. Да Вейга, Дж. Елофф, Ч. Менг, Ю. Чжан. Водночас в умовах російсько-української війни постають принципово нові загрози у сфері інформаційної безпеки держави.

Мета і завдання дослідження

Мета статті полягає в тому, щоб визначити основні загрози інтересам держави у сфері інформаційної безпеки України. Задля досягнення вказаної мети необхідно вирішити такі *завдання*: проаналізувати наявні в науці погляди на сутність особистих, суспільних та державних інтересів; визначити актуальні напрями впровадження нових інформаційних технологій; виокремити основні загрози інтересам держави у сфері інформаційної безпеки України та шляхи їх усунення.

Наукова новизна дослідження

Уперше у вітчизняній правовій доктрині визначено основні загрози інтересам держави у сфері інформаційної безпеки України та наведено авторський підхід до їх усунення.

Виклад основного матеріалу

На початку дослідження ми з'ясуємо сутність інтересів держави. Так, окремі вітчизняні науковці зазначають, що людиноцентричний підхід у діяльності суб'єктів владних повноважень ґрунтується на забезпеченні та захисті прав, свобод і законних інтересів громадян. Саме інтереси людей, які відповідають чинному законодавству і виражають свободу суспільства, визначають зміст і спрямованість діяльності суб'єктів владних повноважень [4].

Водночас у сфері діяльності держави інтереси окремих осіб є похідними від інтересів суспільства в цілому, а інтереси публічних службовців – від мети та завдань органів публічної влади, що охоплюють

встановлені державою загальнообов'язкові правила та стандарти поведінки. Зокрема, як зауважують дослідники з питань антикорупційної діяльності, в основі конфлікту інтересів лежить особистий інтерес публічного службовця, який виявляється в отриманні певних переваг, сприянні підприємницькій діяльності, просуванні корисних осіб тощо, що суперечить засадам виконання публічними службовцями своїх обов'язків та створює значні корупційні ризики [5].

Так, ми підходимо до того, що для осмислення феномена державних інтересів необхідно розкрити сутність суспільних інтересів, які визнаються окремими науковцями ціннісною основою та атрибутом формування державної політики [6, p. 841]. Суспільний інтерес, як стверджує Ч. Менг, визначає стандарти та цілі людських груп, що є ціннісною основою існування державного управління. Публічних службовців вважають головними суб'єктами публічної служби, які приймають рішення та реалізують суспільні інтереси. Однак у практиці публічного управління приватні інтереси інколи порушуються в ім'я суспільних інтересів [7, p. 311]. Подібні описані науковцем обмеження приватних інтересів задля забезпечення національної безпеки мають місце в умовах дії правового режиму воєнного стану в Україні.

Авторський колектив під керівництвом Т. Кагановської до основних ознак суспільного інтересу відносить: сукупність певних потреб (цінностей); можуть існувати потреби всього суспільства, а також його груп чи окремих громадян; ці інтереси визнані державою, можуть бути нормативно закріплені, спрямовані на забезпечення прав і свобод людини, надаються суб'єктами публічного управління. Зміст публічного інтересу як адміністративно-правової категорії випливає із сутності загального інтересу й індивідуалізується змістом адміністративно-правових відносин [4].

Так, на наше глибоке переконання, феномен державних інтересів втілює взаємозв'язок суспільних інтересів та встановленої на нормативно-правовому й організаційно-управлінському рівні специфіки їх реалізації органами публічної влади з урахуванням економічних, соціальних, політичних, дипломатичних, безпекових, інформаційних основ життєдіяльності держави.

Не випадково нами серед основ існування держави як такої виокремлено інформаційну складову. І. Арістова, О. Брусакова, Д. Кошиков та О. Капля зазначають, що немає суспільства без інформації, оскільки завжди існує потреба в спілкуванні. Сучасне суспільство вимагає впровадження нових інформаційних технологій для задоволення своїх потреб. У наш час сектор високих технологій є однією з найважливіших і швидко мінливих сфер суспільного життя. Глобальний сектор високих технологій акумулює серед іншого значні фінансові, грошові та інші ресурси. Він також визнаний таким, що має

значний вплив майже на всі сфери розвитку як державного, так і приватного секторів [8, p. 119]. Водночас ускладнення соціальних структур і відносин, які все більше базуються на сучасних цифрових технологіях, продовжує спричиняти експоненціальне зростання потоків даних [9, p. 60]. Вітчизняні вчені-цивілісти стверджують, що такий розвиток технологій, глобальна комп'ютеризація, міжнародна торгівля призвели до широкого використання інформації, яка стала одним із головних і значущих об'єктів ринкового та цивільного обороту [10, p. 301].

Водночас, попри економічні та соціальні переваги нових інформаційних технологій, за високої динамічності сучасного життя можуть виникнути нові загрози та виклики в національному та глобальному контекстах [11, p. 117].

Одним з основних таких викликів у контексті інтересів держави є забезпечення інформаційної безпеки в новітніх умовах. Адже країна-агресор постійно намагається впливати на вітчизняний інформаційний простір, формувати серед населення ідеї та політичні наративи, спрямовані на дискредитацію чинної влади та всебічну критику поточних державотворчих процесів.

Авторський колектив під керівництвом І. Зозулі під інформаційною безпекою розуміє фундаментальну складову безпеки інформаційно-комунікаційного простору держави, що визначається станом захищеності життєво важливих інтересів людини, суспільства і держави. Змістовна відмінність «життєвих інтересів» є підставою для поділу інформаційної безпеки як єдиної соціально-правової категорії на інформаційну безпеку людини, суспільства і держави [12, p. 747].

Задля більш комплексного розуміння основних загроз інтересам держави у сфері інформаційної безпеки України нами була здійснена спроба виокремлення та аналізу деяких із них.

1. Використання інформаційного впливу задля викривлення політичної думки та ставлення населення до тих чи інших явищ, процесів, органів державної влади, політичних сил та конкретних осіб. Окремі вітчизняні дослідники цієї проблематики переконані, що використання інформаційного впливу може стати фактором розвитку політичної думки та призвести до впровадження певних шкідливих тенденцій. Ключовою метою будь-якої інформаційної війни є зміна політичної думки та дискредитація ідеології і принципів функціонування певного соціального середовища [13, p. 918]. Як приклад науковці наводять використання росією мовних спекуляцій, що триває з 2014 року. Крім того, країна-агресор проводить політику дискредитації української влади за допомогою соціальних платформ, медіа та інструментів забезпечення для того, щоб на її боці в українському просторі були прихильні політичній владі сили. Між Китаєм і США

також тривалий час ведеться інформаційна війна, яка використовує жорстку риторику та матеріали, що дискредитують, на міжнародному рівні [13, p. 918].

2. Недосконале нормативно-правове забезпечення інформаційної безпеки держави. Окремі дослідники конституційного та міжнародного права переконані, що сучасний інформаційний віртуальний простір локальних і глобальних комунікацій вимагає забезпечення певних стандартів доступу якомога більшої кількості громадян до новітніх інформаційно-комунікаційних технологій. Деякі суспільства і держави формують (з певними характерними відмінностями національних моделей) принципово новий правовий механізм реалізації основних інформаційних прав і свобод [14]. Слід зауважити, що важливість забезпечення інформаційної безпеки в державі закріплена на міжнародному рівні, зокрема резолюції ООН діють фактично в кожній країні світу і мають чіткі положення про інформаційну війну й основні засоби протидії їй [13, p. 919]. Пошук шляхів вирішення цієї загрози лежить у площині розробки комплексного нормативно-правового акта про засади інформаційної безпеки України, який закріпив би реальні та потенційні загрози інформаційній безпеці, основи державної політики у сфері інформаційної безпеки, зокрема в умовах воєнного стану, що сприяло б подальшому розвитку цієї сфери, узгодженості окремих підзаконних нормативно-правових актів, які частково регулюють цю сферу та закладають стратегічне бачення її розвитку.

3. Навмисне викривлення інформації на рівні лідерів держав і дипломатичних представників та їх негативний вплив на думку міжнародної спільноти. Так, важливим фактором інформаційної війни є підтримка сторін таких кампаній, що ускладнює протидію інформаційним атакам. Зокрема, спільна риторика Китаю та росії щодо фіктивного мирного врегулювання війни в Україні є ключовим напрямом для проведення інформаційних атак на весь світ. Питання продовольчої безпеки в Африці, використання європейської енергетичної кризи, постачання зброї із США є ключовими інструментами інформаційної війни росії [13, p. 919].

4. Недостатня участь населення України у протидії інформаційним атакам. Ця загроза постає у світлі необхідності використання потенціалу сучасних інформаційних технологій у процесі поширення населенням інформації про реальні проблеми та потреби в Україні на низовому рівні. Сучасні месенджери та соціальні мережі дозволяють конкретній особі охопити аудиторію у сотні тисяч та мільйонів осіб і миттєво донести міжнародній спільноті справжні, а не штучно сформовані настрої та ідеї населення щодо тих чи інших проблем, пов'язаних із патріотизмом і відданістю державі. Особливим потенціалом у

цьому контексті наділена інтелектуальна еліта суспільства, зокрема митці і творчі особистості, які здатні передати у своїх творах чи виступах образи та картини життя українського суспільства в умовах російсько-української війни.

5. Недосконалість інституційного й організаційного забезпечення освіти з інформаційної безпеки та формування культури інформаційної безпеки в суспільстві. Впровадження такої освіти серед широких верств населення є необхідним у сучасних реаліях поряд із бойовою підготовкою, адже дозволяє озброїти населення комплексом необхідних знань про основи критичного мислення, інформаційну гігієну та безпеку в медіапросторі.

Розвиток культури інформаційної безпеки в державі можна простежити на рівні конкретної організації. Так, А. Да Вейга та Дж. Елофф зазначають, що культура інформаційної безпеки розвивається в організації завдяки певним діям. Керівництво впроваджує такі компоненти інформаційної безпеки, як правила і технічні заходи безпеки, які співробітники застосовують у своїх робочих процедурах. Співробітники розвивають певні уявлення та поведінку, наприклад звітування про інциденти безпеки або обмін паролями, що може або сприяти, або становити загрозу безпеці інформаційних активів [15, p. 361]. Водночас окремі дослідники більш широко досліджують критичні фактори успіху культури інформаційної безпеки: підтримка інформаційної безпеки з боку вищого керівництва, створення ефективної політики інформаційної безпеки, обізнаність у сфері інформаційної безпеки, навчання та освіта з інформаційної безпеки, аналіз і оцінка ризиків інформаційної безпеки, відповідність вимогам інформаційної безпеки, політика етичної поведінки та організаційна культура [16, p. 731].

У межах держави розвиток культури інформаційної безпеки може бути втілений шляхом розробки загальнонаціональних стратегій, які б охоплювали комплекси заходів освітнього, світоглядного, культурного характеру, а також різні категорії населення, наприклад, розроблення системи підвищення кваліфікації для публічних службовців, викладання окремих дисциплін для здобувачів закладів вищої освіти та проведення занять, конкурсів, турнірів для учнів закладів загальної середньої освіти.

Висновки

Підсумовуючи вищевикладене, можна дійти висновку, що в умовах значного впливу інформації на життя суспільства одними з основних загроз, які постають перед сучасними державами, виступають саме інформаційні.

З огляду на це у наш час мають місце повномасштабні інформаційні війни, спрямовані на всебічне перешкоджання нормальному функціонуванню держави в інформаційній сфері, зокрема з початком

російсько-української війни значна увага держави-агресора прикута саме до інформаційної сфери як однієї з базових сфер життєдіяльності українського суспільства.

Феномен державних інтересів утілює взаємозв'язок суспільних інтересів та встановленої на нормативно-правовому й організаційно-управлінському рівнях специфіки їх реалізації органами публічної влади з урахуванням економічних, соціальних, політичних, дипломатичних, безпекових, інформаційних основ життєдіяльності держави.

Водночас, попри економічні та соціальні переваги нових інформаційних технологій, в умовах динамічних перебудов сучасного життя можуть виникнути нові загрози інтересам держави у сфері інформаційної безпеки України. Адже країна-агресор постійно намагається впливати на вітчизняний інформаційний простір, формувати серед населення ідеї та наративи, спрямовані на дискредитацію чинної влади та всебічну критику поточних державотворчих процесів.

Задля більш комплексного розуміння основних загроз інтересам держави у сфері інформаційної безпеки України нами були виокремлено такі загрози: використання інформаційного впливу задля викривлення політичної думки та ставлення населення до тих чи інших явищ, процесів, органів державної влади, політичних сил та конкретних осіб; недосконале нормативно-правове забезпечення інформаційної безпеки держави; навмисне викривлення інформації на рівні лідерів держав і дипломатичних представників та їх негативний вплив на думку міжнародної спільноти; недостатня участь населення України у протидії інформаційним атакам; недосконалість інституційного й організаційного забезпечення освіти з інформаційної безпеки та формування культури інформаційної безпеки в суспільстві.

Задля усунення вищенаведених загроз запропоновано: розробити комплексний нормативно-правовий акт про засади інформаційної безпеки України, який закріпив би реальні та потенційні загрози інформаційній безпеці, основи державної політики у сфері інформаційної безпеки, зокрема в умовах воєнного стану, що сприяло б подальшому розвитку цієї сфери, узгодженості окремих підзаконних нормативно-правових актів, які частково регулюють цю сферу та закладають стратегічне бачення її розвитку; використовувати потенціал сучасних інформаційних технологій у процесі поширення населенням інформації про реальні проблеми та потреби на низовому рівні, доносити міжнародній спільноті справжні, а не штучно сформовані настрої та ідеї населення щодо тих чи інших проблем, пов'язаних із патріотизмом та відданістю державі; впроваджувати освіту з інформаційної безпеки, що дозволяє озброїти населення комплексом необхідних знань про основи критичного мислення, інформаційну

гігієну та безпеку в медіапросторі; розвивати культуру інформаційної безпеки шляхом розробки загальнонаціональних стратегій, які б охоплювали комплекси заходів освітнього, світоглядного, культурного характеру, а також різні категорії населення, наприклад розроблення системи підвищення кваліфікації для публічних службовців, викладання окремих дисциплін для здобувачів закладів вищої освіти та проведення занять, конкурсів, турнірів для учнів закладів загальної середньої освіти.

Список бібліографічних посилань: 1. Brusakova O., Shayturo O., Simonovych D., Kuzubova T. Submission of a Civil Suit by a Prosecutor in the Interests of a State as a Way of Compensation for Damage Caused by a Criminal Offence. *Jurnal Cita Hukum*. 2021. Vol. 9, No. 1. Pp. 63–76. DOI: https://doi.org/10.15408/jch.v9i1.19793. **2.** Manzhai O., Kuryliuk Yu., Miroshnykov I., Syiploki M., Vazhynskyi V. Criminal and legal protection of information relations. *International Journal of Computer Science and Network Security*. 2022. Vol. 22, No. 5. Pp. 284–288. DOI: https://doi.org/10.22937/ijcsns.2022.22.5.39. **3.** Holubieva V., Pravdiuk A., Oliinyk S., Manzhai O., Shynkar T. Constitutional and legal provision of the right to access information in Ukraine and the countries of the European Union. *AD ALTA: Journal of Interdisciplinary Research*. 2022. Vol. 12, Iss. 1. Pp. 156–159. **4.** Kaganovska T. E., Pakhomova I. A., Neviadovskyi V. O., Yefremov A. O. Public interest as a category of administrative and legal science. *Ius Humani. Revista De Derecho*. 2022. Vol. 11 (1). DOI: https://doi.org/10.31207/ih.v11i1.292. **5.** Zhuravel O. Ye., Bezusa Yu. O., Lubentsov A. V., Ternytskyi S. M., Tykhonova D. S. Conflict of interests in the CIS countries: A comparative analysis. *Journal of Legal, Ethical and Regulatory Issues*. 2019. Vol. 22, Iss. 5. URL: https://www.abacademies.org/articles/Conflict-of-interests-in-the-CIS-countries-a-comparative-analysis-1544-0044-22-5-403.pdf (дата звернення: 19.01.2024). **6.** Zhang Y. Public interest interpretation from policy-making perspective // 6th International Conference on Public Administration (Canberra, 22–24 October 2010). Canberra : Australian National University, 2010. Pp. 841–847. **7.** Meng Q. Analysis restrictions against the abuse of public interest in public administration // 4th International Conference on Public Administration (Minneapolis, 24–26 September 2008). Minneapolis : University of Minnesota, 2008. Pp. 311–316. **8.** Aristova I., Brusakova O., Koshikov D., Kaplya O. Developing information technology law and legislation: Analysis of international experience and possibilities of its application in Ukraine. *Ius Humani. Revista de Derecho*. 2021. Vol. 10 (2). Pp. 117–128. DOI: https://doi.org/https://doi.org/10.31207/ih.v10i2.287. **9.** Andriushchenko K., Rudyk V., Riabchenko O., Kachynska M., Marynenko N., Shergina L., Kovtun V., Tepliuk M., Zhemba A., Kuchai O. Processes of managing information infrastructure of a digital enterprise in the framework of the "Industry 4.0" concept. *Eastern-European Journal of Enterprise Technologies*. 2019. Vol. 1/3 (97). Pp. 60–72. DOI: https://doi.org/

10.15587/1729-4061.2019.157765. **10.** Iasechko S., Haliantych M., Skomorovskyi V., Zadorozhnyi V., Obryvkina O., Pohrebniak O. Contractual Relations in the Information Sphere. *Systematic Reviews in Pharmacy*. 2020. Vol. 11, Iss. 8. Pp. 301–303. DOI:-https://doi.org/10.31838/srp.2020.8.46. **11.** Shumilo O., Anisimova H., Shekhovtsov V., Kobko Ye. Modern legislation to protect the environmental interests of citizens: new challenges in the context of armed conflict in Ukraine. *Lex Humana*. 2022. Vol. 14, No. 2. Pp. 107–120. **12.** Zozulia I., Zozulia O., Yukhno O., Panova I., Krykun V. Ensuring Information security as a function of the modern state: the experience of Ukraine. *International Journal of Computer Science and Network Security*. 2022. Vol. 22, No. 5. Pp. 747–756. DOI: https://doi.org/10.22937/IJCSNS.2022.22.5.102. **13.** Cherniavska B., Shevchenko S., Kaletnik V., Dzhahupov H., Madryha T. Information Warfare in the World and Information Security Issues in the Context of the Russian-Ukrainian War. *Review of Economics and Finance*. 2023. Vol. 21, No. 1. Pp. 916–922. DOI: https://doi.org/10.55365/1923.x2023.21.100. **14.** Voitsikhovskyi A., Bakumov O., Ustymenko O., Syroid T. The right of access to the internet as fundamental human right given the development of global information society. *The Law, State and Telecommunications Review*. Vol. 13, No. 1. DOI: https://doi.org/10.26512/lstr.v13i1.30904. **15.** Da Veiga A., Eloff J. An information security governance framework. *Information Systems Management*. 2007. Vol. 24, Iss. 4. Pp. 361–372. DOI: http://doi.org/10.1080/10580530701586136. **16.** Alnatheer M. Information Security Culture Critical Success Factors // Information Technology: New Generations 2015 : proceedings of the Twelfth International Conference on Information Technology (Las Vegas, NV, USA, 13–15 April 2015). Las Vegas, 2015. Pp. 731–735. DOI: https://doi.org/10.1109/ITNG.2015.124.

Надійшла до редколегії 22.01.2024

Прийнята до опублікування 05.02.2024

Starostin O. Yu. Main threats to the state's interests in the sphere of information security of Ukraine

The article emphasises that in the context of the significant impact of information on society, one of the main threats faced by modern states is information.

It is noted that the phenomenon of the State interests embodies the interconnection of public interests and the specifics of their implementation by public authorities established at the regulatory, legal, organisational and administrative levels, taking into account the economic, social, political, diplomatic, security and information foundations of the State's vital activity.

For the purpose of more comprehensive understanding of the main threats to the interests of the state in the field of information security of Ukraine, the following threats are identified: the use of information influence to distort political opinion and attitudes of the population to certain phenomena, processes, public authorities, political forces and individuals; imperfect

regulatory and legal support for the information security of the state; deliberate distortion of information at the level of state leaders and diplomatic representatives and their negative impact on the opinion of the international community; insufficient participation of the Ukrainian population in countering information attacks; insufficient institutional and organisational support for information security education and the formation of an information security culture in society.

In order to eliminate the above threats, it is proposed to: develop a comprehensive legal act on the principles of information security of Ukraine, which would consolidate real and potential threats to information security, the foundations of the State policy in the field of information security, in particular under martial law, which would facilitate further development of this area, consistency of certain by-laws and regulations that partially regulate this area and lay down a strategic vision of its development; use the potential of modern information technologies in the process of disseminating information about real problems and needs at the grassroots level; convey to the international community the real, not artificially formed, moods and ideas of the population regarding certain problems related to patriotism and loyalty to the state; introduce information security education, which allows equipping the population with a set of necessary knowledge about the basics of critical thinking, information hygiene and media security; In order to eliminate the above threats, it is proposed to: develop a culture of information security by developing national strategies that would cover a set of educational, ideological, cultural activities, as well as different categories of the population, for example, developing a system of professional development for public servants, teaching certain disciplines for students of higher education institutions and holding classes, competitions, tournaments for students of general secondary education institutions.

Key words: information security, state interests, main threats, information warfare.