УДК 342.92
DOI: https://doi.org/10.17721/1728-2217.2022.50.95-98

С. Онопрієнко, канд. юрид. наук
ORCID ID 0000-0002-5524-1798
Київський національний університет імені Тараса Шевченка, Київ, Україна

ФУНКЦІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ В УКРАЇНІ ЗА УМОВ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Визначено поняття і види функцій забезпечення інформаційної безпеки публічного адміністрування в Україні за умов повномасштабної збройної агресії російської федерації. Це притаманні діяльності публічних адміністрацій способи збереження власної функціональності за умов деструктивних інформаційних впливів і попередження спричинення шкоди (небезпеки) інформаційним правам та інтересам людини, громадянського суспільства, органів, підприємств, установ та організацій і державі в цілому. На основі контентного аналізу діяльності публічних адміністрацій в інформаційній сфері виокремлено такі стадії реалізації функцій забезпечення інформаційної безпеки публічного адміністрування: 1) констатації та узагальнення; 2) аналізу; 3) моделювання; 4) нормативного закріплення; 5) практичної реалізації; 6) рефлексії та оцінювання. Охарактеризовано вказані стадії. Обґрунтовано, що функції забезпечення інформаційної безпеки публічного адміністрування можна класифікувати за різними критеріями, проте доцільнішою є класифікація за критерієм результативності. Запропоновано класифікацію, що містить функцію збереження інформаційного суверенітету; функцію інформування міжнародного співтовариства щодо порушення противником законів і звичаїв війни, спричинення шкоди здоров'ю, життю та майну цивільного населення; функцію виховання високого рівня інформаційної культури; функцію консолідації. Надано характеристику і визначено особливості реалізації цих функцій за умов дії правового режиму воєнного стану. Зроблено висновок, що функції забезпечення інформаційної безпеки публічного адміністрування є одними з пріоритетних з-поміж інших функцій забезпечення національної безпеки. Відмінність реалізації означених функцій за умов повномасштабної збройної агресії російської федерації полягає в тому, що первинним на сьогодні є застосування кінетичної зброї. Однак можливість України вистояти та ефективно протистояти російській агресії істотно залежить від вміння та вдалого застосування функції інформування міжнародного співтовариства щодо порушення противником законів і звичаїв війни, спричинення шкоди здоров'ю, життю та майну цивільного населення. Зберігає свою актуальність функція виховання високого рівня інформаційної культури, що унеможливлює руйнівний вплив противника на життєдіяльність держави і громадянського суспільства.

Ключові слова: інформаційна безпека, національна безпека, функції, стадії, інформаційні правовідносини, повномасштабна збройна агресія російської федерації.

Постановка проблеми. Повномасштабна збройна агресія російської федерації поставила перед суб'єктами забезпечення інформаційної безпеки України невідкладні завдання, пов'язані із захистом інформаційного суверенітету, зниженням руйнівного впливу наративів, активно використовуваних противником для деструктивного впливу на функціонування публічних адміністрацій і на морально-психологічний стан населення тимчасово окупованих територій. Ці завдання нагальні, і відкладення їх вирішення на інший, більш сприятливий час, як засвідчив восьмирічний досвід протистояння збройній агресії рф, лише збільшує та ускладнює існуючі проблеми. На жаль, відсутність системності та комплексності у сфері інформаційної безпеки не дозволяє побудувати ефективну систему протидії деструктивним інформаційним впливам противника. Безумовно, сьогодні можна констатувати певні здобутки на шляху подолання інформаційних ризиків, хоча вони радше залежать від активної роботи окремих органів публічного адміністрування, – Офісу Президента України, прес-служб ЗСУ, Міністерства оборони України, Служби безпеки України, деяких представників органів місцевого самоврядування. Проте на загальнодержавному рівні єдина стратегія забезпечення інформаційної безпеки за умов повномасштабної російської збройної агресії поки відсутня. Це ставить перед дослідниками завдання щодо вироблення теоретико-методологічної бази, яка могла б бути використана під час прийняття відповідних політичних та організаційно-управлінських рішень. Вказане обумовлює актуальність і важливість дослідження сутності функцій забезпечення інформаційної безпеки публічного адміністрування в умовах повномасштабного збройного конфлікту.

Аналіз останніх досліджень і публікацій. Питання, пов'язані із сутністю та складовими інформаційної безпеки, розглядали у своїх роботах такі вчені, як І. Арістова, О. Баранов, К. Бєляков, В. Глушков, О. Довгань, О. Золотар, Р. Калюжний, Б. Кормич, А. Марущак, Н. Новицька, О. Олійник, В. Петрик, В. Пилипчук, В. Полевий, Л. Радовецька, Є. Скулиш, О. Тихомиров, Т. Ткачук, В. Цимбалюк, В. Фурашев, О. Шевчук та інші. Проте функції забезпечення інформаційної безпеки за умов повномасштабної збройної агресії російської федерації ще не знайшли свого достатнього висвітлення на науково-теоретичному рівні, що зумовлює напрями подальших наукових пошуків.

Мета статті – визначення поняття та видів функцій забезпечення інформаційної безпеки публічного адміністрування в Україні за умов повномасштабної збройної агресії російської федерації.

Виклад основного матеріалу. Відносини у сфері забезпечення інформаційної безпеки органів публічного адміністрування мають публічно-правовий характер, оскільки пов'язані з виконанням державою своїх функцій, спрямованих на захист інформаційного суверенітету, забезпеченням інформаційних прав і свобод учасників правовідносин. Слід погодитися з Л. Радовецькою, яка вважає, що забезпечення інформаційної безпеки є функцією держави, оскільки цій правовій категорії характерні такі змістові характеристики, які є іманентними ознаками для поняття функція держави: це об'єктивні, найбільш важливі напрями діяльності; через поняття функції розкривається соціальне призначення держави в суспільстві; через поняття функції конкретизуються завдання держави, її призначення; функції держави втілюються у життя не самі по собі, а за допомогою державних органів, громадян та інших суб'єктів практичної діяльності [1,

ISSN 1728-2217

с. 13]. Зауважимо, що не можна ототожнювати функції держави і функції забезпечення інформаційної безпеки, оскільки коло суб'єктів забезпечення інформаційної безпеки значно ширше і містить велику кількість недержавних (неурядових) суб'єктів, від органів місцевого самоврядування до інститутів громадянського суспільства.

Термін "функція" у загальному розумінні визначається як основний напрям, сфера, ділянка діяльності, характерна властивість, притаманна певному предмету або явищу, його провідна ознака, що виступає метою та сенсом існування об'єкта. Як справедливо зауважує М. Матійко, термін "функція" досить багатомірний, він придатний для характеристики будь-яких динамічних структур. У філософських дослідженнях функція – це відношення двох (групи) об'єктів, у якому зміна одного з них веде до зміни іншого. Функція може розглядатися з точки зору наслідків (сприятливих, несприятливих – дисфункціональних або нейтральних афункціональних), які викликаються зміною одного параметра в інших параметрах об'єкта (функціональність), або взаємозв'язку окремих частин у межах якогось цілого (функціонування) [2, с. 221].

Отже, терміни "функція" і "функціонування" нерозривно пов'язані і, якщо функція являє собою характеристику об'єкта в певний момент часу, в умовній статиці, обумовленій часовим зрізом, то функціонування є динамічною характеристикою об'єкта.

Слід також сказати, що функції забезпечення за своєю правовою природою відмінні від функцій права. Функції права, з тими чи іншими відмінностями, зазвичай розуміють як прояв його іманентних, специфічних властивостей. У функції акумулюються такі властивості права, що випливають з її якісною самостійності як соціального феномена. При цьому вважається, що функція права випливає з її сутності і визначається призначенням права в суспільстві [3, с. 46]. Натомість, забезпечення є характеристикою діяльності як активності публічних адміністрацій, спрямованої на досягнення їх визначених законами та підзаконними правовими актами цілей та завдань.

На підставі вказаного вище пропонуємо визначення функцій забезпечення інформаційної безпеки публічного адміністрування в Україні – це притаманні діяльності публічних адміністрацій способи збереження власної функціональності за умов деструктивних інформаційних впливів і попередження спричинення шкоди (небезпеки) інформаційним правам та інтересам людини, громадянського суспільства, органів, підприємств, установ та організацій і держави в цілому.

На основі контентного аналізу діяльності публічних адміністрацій в інформаційній сфері можна виокремити такі стадії реалізації функцій забезпечення інформаційної безпеки публічного адміністрування:

- стадія констатації та узагальнення призначена для визначення існуючих інформаційних загроз, накопичення інформації щодо них та виявлення спільних властивостей. Вказана стадія дозволяє від трансцендентного сприйняття інформаційних загроз перейти до їх аналізу, що базується на підтверджених фактах спричинення або спроби спричинення шкоди інформаційним правовідносинам.
- стадія аналізу дозволяє виявити і структурувати притаманні об'єкту закономірності, скласти ієрархію найбільш значущих з них, виявити періодичність, джерело, форми розповсюдження найбільш значущих інформаційних загроз, їхню мету, спрямованість та особливості керованості;
- стадія моделювання дає змогу визначити найбільш вразливі точки інформаційної діяльності противника щодо продукування інформаційних загроз і підготувати оптимальні засоби та способи її припинення або ослаблення (зниження ефективності);
- стадія нормативного закріплення передбачає прийняття управлінського рішення щодо включення оптимальних способів і засобів припинення інформаційної діяльності противника до актуальних завдань та комплексу оперативних дій публічної адміністрації й інших суб'єктів забезпечення інформаційної безпеки, а також закріплення вказаного рішення у відповідних нормативних і правових актах;
- стадія практичної реалізації функцій забезпечення інформаційної безпеки публічного адміністрування включає безпосереднє здійснення визначених у нормативних та правових актах завдань, дій і засобів для подолання інформаційних ризиків та загроз;
- стадія рефлексії та оцінювання дозволяє визначити ефективність діяльності на попередніх стадіях і скоригувати майбутню діяльність у сфері інформаційної безпеки для збільшення її ефективності.

Вказані стадії зазвичай реалізуються послідовно, проте не можна не згадати про випадки, коли внаслідок недоліків в організації та плануванні або через дефіцит часу, викликаного підвищеною небезпекою певної інформаційної загрози, певні стадії можуть бути пропущені. На нашу думку, це сприяє збільшенню хаотичності у функціонуванні системи забезпечення інформаційної безпеки.

Функції забезпечення інформаційної безпеки публічного адміністрування можна класифікувати за різними критеріями, проте доцільнішою нам видається класифікація за критерієм результативності.

Функція збереження інформаційного суверенітету – це спроможність системи публічного адміністрування управляти процесами зовнішніх інформаційних впливів, даючи відсіч деструктивним інформаційним способам спричинити шкоду національній безпеці держави та інтересам громадянського суспільства.

Функція інформування міжнародного співтовариства щодо порушення противником законів і звичаїв війни, спричинення шкоди здоров'ю, життю та майну цивільного населення передбачає випередження руйнівного впливу фейків та інших способів спотворення об'єктивної інформації щодо ведення бойових дій та поводження з цивільними особами. Таке випередження досягається завдяки активній роботі публічних адміністрацій щодо оприлюднення на широкий міжнародний загал фактів, які характеризують дії противника.

Функція виховання високого рівня інформаційної культури обумовлює створення органами публічного адміністрування умов для найповнішого оволодіння їх персоналом, а також широкими верствами громадян знаннями, вміннями та навичками, які унеможливлюють вразливість системи публічного адміністрування та суспільства від інформаційних атак противника, у тому числі кібератак. За умов повномасштабної збройної агресії російської федерації таке унеможливлення вразливості виступає однією із складових кібероборони – сукупності політичних, економічних,

соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі і спрямовані на забезпечення захисту суверенітету й обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [4].

Функція консолідації – це спрямованість зусиль публічних адміністрацій на створення загальнонаціонального консенсусу, що передбачає об'єднання різних суб'єктів забезпечення інформаційної безпеки на основі усвідомлення загальної мети, толерантності та взаємоповаги. З цього приводу хотілося б зробити деякі зауваження щодо розуміння сутності такої взаємодії у правовій та демократичній державі. Деякі дослідники вважають, що людина і громадянин і демократичне суспільство в цілому зобов'язані відповідати уявленням держави про силу, спрямованість і періодичність їхньої громадянської активності в інформаційній сфері. Інакше кажучи, держава формулює цілі та способи дій, а громадяни зобов'язані безоплатно та беззастережно прикладати максимум зусиль для досягнення таких цілей. Наприклад, А. Головка пише, що в сучасних умовах інститути громадянського суспільства є повноцінними учасниками процесу забезпечення інформаційної безпеки України. Як показує суспільно-політична практика, зусиль держави зазвичай не вистачає для ефективної протидії інформаційним загрозам. Це, у свою чергу, змушує вище державне керівництво формувати діалог із інститутами громадянського суспільства, які виступають у ролі надійних союзників держави. Разом з тим, у взаємодії між громадянським суспільством та державою в Україні є ряд проблемних питань. Ідеться насамперед про наявність скептичних настроїв серед населення щодо можливості реального впливу на прийняття політичних рішень у секторі безпеки; недосконалість інституційної бази; брак досвіду взаємодії громадянського суспільства та держави в умовах інформаційної війни; недосконалість українського законодавства. Основними шляхами вирішення цих проблем є результативна інформаційна політика держави та громадського сектору в напрямі формування активістського типу політичної культури українського суспільства, а також вдосконалення інституційної та нормативно-правової бази. Виходячи із перерахованих вище проблем, автор робить висновок, що ефективність механізмів залучення громадянського суспільства до безпекової політики в інформаційній сфері поки що далека від оптимальної. Окремі індивіди, соціальні групи та українське суспільство в цілому повинні будувати активістський тип політичної культури та максимально використовувати всі доступні засоби впливу на прийняття політичних рішень у секторі безпеки [5, с. 95-96]. Застосування до людини та громадського суспільства терміну "повинні" у контексті формування їхньої громадської активності уявляється нам некоректним і притаманним ідеології тоталітарної держави. Людина і громадянин, окремі інститути громадянського суспільства проявляють свою активність у той момент і спосіб, які самі вважають доцільними (якщо така активність не порушує законодавчі приписи). Примушення до громадської активності в демократичному суспільстві неприпустиме, а отже, сутність функції консолідації включає збирання інформації щодо позицій недержавних суб'єктів забезпечення інформаційної безпеки та пошук спільних підстав сумісної з ними діяльності. Окрім того, зауважимо, що за умов правового режиму воєнного стану має місце обмеження деяких прав і свобод людини та громадянина, у тому числі в інформаційній сфері, яке, безумовно, може здійснюватися лише на підставі Конституції та законів України. Такі обмеження мають бути враховані під час побудови концепції консолідації громадянського суспільства і публічних адміністрацій у сфері забезпечення інформаційної безпеки.

Висновки. На підставі вказаного вище можна зробити висновок, що функції забезпечення інформаційної безпеки публічного адміністрування є одними з пріоритетних з-поміж інших функцій забезпечення національної безпеки. Відмінність реалізації означених функцій за умов повномасштабної збройної агресії російської федерації полягає в тому, що первинним на сьогодні є застосування кінетичної зброї. Однак можливість України вистояти та ефективно протистояти російській агресії значним чином залежить від вміння та вдалого застосування функції інформування міжнародного співтовариства щодо порушення противником законів і звичаїв війни, спричинення шкоди здоров'ю, життю та майну цивільного населення. Окрім того, зберігає свою актуальність функція виховання високого рівня інформаційної культури, що унеможливлює руйнівний вплив противника на життєдіяльність держави і громадянського суспільства.

Список використаних джерел

1. Радовецька Л.В. Місце інститутів громадянського суспільства у механізмі реалізації функції забезпечення інформаційної безпеки // Інформаційна безпека людини, суспільства, держави, 2013. № 3. С. 12–18.

2. Матійко М.В. Інформаційна функція цивільного права // Актуальні проблеми держави і права, 2008. № 45. С. 199–204.

3. Ісаєва В.В. Функції права: теоретико-правовий аналіз // Часопис Київського університету права, 2013. № 1. С.45–48.

4. Головка А.А. Вдосконалення механізмів залучення громадянського суспільства до реалізації політики безпеки у інформаційній сфері України // Наук.-інформ. вісн. Академії нац. безпеки, 2016. № 1-2. С. 86–98.

5. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 11.05.2022).

References

1. Radovetskaya, L.V. (2013). The place of civil society institutions in the mechanism of implementation of the information security function. *Information security of man, society, state*, volume 3, .pp. 12-18. [in Ukrainian].

2. Matiyko, M.V. (2008). Information function of civil law. *Current issues of state and* law, volume 45, pp.199-204. [in Ukrainian].

3. Isaeva, V.V. (2013). Functions of law: theoretical and legal analysis. *Journal of Kyiv University of Law*, volume 1, pp.45-48. [in Ukrainian].

4. Golovka, A.A. (2016) Improving the mechanisms of involving civil society in the implementation of security policy in the information sphere of Ukraine. Scientific and Information Bulletin of the Academy of National Security, volume 1-2, pp. 86-98. [in Ukrainian].

5. On the basic principles of cybersecurity of Ukraine: Law of Ukraine of October 5, 2017 № 2163-VIII. https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

Надійшла до редколегії 12.05.22

S. Onopriienko, PhD of Judical Sci.
ORCID ID 0000-0002-5524-1798
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

FUNCTIONS OF ENSURING INFORMATION SECURITY OF PUBLIC ADMINISTRATION IN UKRAINE IN THE FACE OF FULL-SCALE ARMED AGGRESSION OF THE RUSSIAN FEDERATION

The purpose of the article is to define the concept and functions of ensuring the information security of public administration in Ukraine in the conditions of full-scale armed aggression of the Russian Federation. The definition is proposed for the functions of ensuring the information security of public administration in Ukraine: these are the methods inherent in the activities of public administrations to preserve their own functionality in the face of destructive information influences and prevent harm (danger) to the information rights and interests of a person, civil society, bodies, enterprises, institutions and organizations and the state generally. Based on the content analysis of the activities of public administrations in the information sphere, the following stages of implementation of the functions of ensuring information security of public administration have been identified: 1) statements and generalizations; 2) analysis; 3) modeling; 4) regulatory consolidation; 5) practical implementation; 6) reflection and evaluation. These stages are characterized. The substantiation of the thesis is given that the functions of ensuring information security of public administration can be classified according to different criteria, but it is more appropriate to classify according to the criterion of effectiveness. The classification is proposed, which includes: the function of maintaining information sovereignty, the function of informing the international community about the enemy's violation of the laws and customs of war, causing harm to the health, life and property of the civilian population; the function of educating a high level of information culture; consolidation function. The characteristic is provided by the specified functions. Features are defined for the implementation of these functions in the conditions of the legal regime of martial law. The conclusion is made that the functions of ensuring the information security of public administration are one of the priorities among other functions of ensuring national security. Arguments are given that the ability of Ukraine to withstand and effectively resist Russian aggression significantly depends on the ability and successful application of the function of informing the international community about the enemy's violation of the laws and customs of war, causing harm to the health, life and property of the civilian population. In addition, the function of educating a high level of information culture remains relevant, which makes it impossible for the enemy to have a destructive influence on the life of the state and civil society.

Keywords: information security, state security, functions, stages, information legal relations, full-scale armed aggression of the Russian Federation.