

Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019).

Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2022. № 12.

DOI: <http://doi.org/10.32702/2307-2156.2022.12.6>

УДК 351.74: 075.2

Я. П. Цецик,

к. і. н., доцент кафедри публічного управління, адміністрування та інформаційної діяльності, Національний університет водного господарства та природокористування

ORCID ID: <https://orcid.org/0000-0002-2527-2155>

В. І. Корбутяк,

к. т. н., доцент кафедри публічного управління, адміністрування та інформаційної діяльності, Національний університет водного господарства та природокористування).

ORCID ID: <https://orcid.org/0000-0002-2252-3801>

С. П. Цецик,

к. пед. н., доцент кафедри вищої математики, Національний університет водного господарства та природокористування

ORCID ID: <https://orcid.org/0000-0001-7047-4197>

ОСОБЛИВОСТІ УПРАВЛІННЯ ДІЯЛЬНІСТЮ ІНФОРМАЦІЙНИХ УСТАНОВ В УМОВАХ ВОЄННОГО ЧАСУ

Ya. Tsetsyk,

PhD in Historical Sciences, Associate Professor of the Department of Public Administration, Documentation and Information Activity, National University of Water Management and Nature Management

V. Korbutiak,

PhD in Technical Sciences, Associate Professor of the Department of Public Administration, Documentation and Information Activity, National University of Water Management and Nature Management

S. Tsetsyk,

PhD in Pedagogical Sciences, Associate Professor of the Department of Higher (Further) Mathematics, National University of Water Management and Nature Management

**FEATURES OF MANAGEMENT OF THE ACTIVITIES OF INFORMATION
INSTITUTIONS IN WARTIME CONDITIONS**

У сучасному суспільстві інформаційні технології відіграють ключову роль, а їхнє застосування охопило всі сфери життєдіяльності. Впродовж останніх десятиліть в Україні діяльність інформаційних установ зазнала кардинальних змін, які стали орієнтованими на забезпечення потреб не лише підприємств та організацій, й громадян. Така ситуація призвела до застосування низки нових методів в управлінні діяльністю інформаційними установами. Державне управління інформаційною сферою незважаючи на його галузевий характер відіграє ключову роль у подальшому її розвитку та координації діяльності. В умовах воєнного часу було змінено підходи до стратегічного управління інформаційними установами, це насамперед пов'язано з необхідністю захищати інформацію, протидіяти кібератакам тощо. Важливим фактором стало забезпечення інформаційними установами, що функціонують у нашій державі ключових потреб пов'язаних із захистом інформації, безпекою критичної інфраструктури.

У зв'язку з цим управління інформаційною установою в умовах воєнного стану серед головних пріоритетів державної політики у галузі інформаційної безпеки виділяють належний рівень захисту головних інформаційних потреб та інтересів суспільства, особистості та держави. Враховуючи наявність загроз національній безпеці України саме на цьому напрямі діяльності зобов'язані сконцентрувати свої зусилля органи влади, які спільно з керівниками інформаційних установ мають протидіяти тим загрозам і викликам, що постали перед нашою державою.

Враховуючи постійне застосування інформаційних технологій у військово-політичних цілях у тому числі й агресії. Тому на сучасному етапі ключове значення приділяється розробці та впровадженню дієвих механізмів прогнозування, виявлення та оцінки інформаційних загроз, нейтралізації інформаційно-психологічного впливу населення країни, в тому числі спрямованого на підриєв національних цінностей та історичної спадщини. У такій ситуації керівники інформаційних установ спільно з органами влади мають застосовувати ефективні методи управління, бути готовими приймати відповідальні рішення, які сприятимуть ефективному вирішенню ключових проблем. У комплексі це сприятиме пошуку оптимальних шляхів вирішення ключових проблем, що постали перед галуззю.

In modern society, information technologies play a key role, and their application has covered all spheres of life. Over the past decades, the activities of information institutions in Ukraine have undergone drastic changes, which have

become oriented towards meeting the needs not only of enterprises and organizations, but also of citizens. This situation led to the application of a number of new methods in the management of the activities of information institutions. State management of the information sphere, despite its sectoral nature, plays a key role in its further development and coordination of activities. In the conditions of wartime, approaches to the strategic management of information institutions were changed, this is primarily due to the need to protect information, counter cyber attacks, etc. An important factor was the provision by information institutions operating in our country of key needs related to information protection and critical infrastructure security.

In this regard, the management of an information institution under martial law among the main priorities of state policy in the field of information security is the appropriate level of protection of the main information needs and interests of society, the individual and the state. Given the existence of threats to the national security of Ukraine, it is precisely in this area of activity that the authorities are obliged to concentrate their efforts, which, together with the heads of information institutions, must counter the threats and challenges that have arisen before our state.

Taking into account the constant use of information technologies for military and political purposes, including aggression. Therefore, at the current stage, key importance is attached to the development and implementation of effective mechanisms for forecasting, identifying and evaluating informational threats, neutralizing the informational and psychological influence of the country's population, including those aimed at undermining national values and historical heritage. In such a situation, the heads of information institutions together with the authorities should apply effective management methods, be ready to make responsible decisions that will contribute to the effective solution of key problems. In the complex, this will contribute to the search for optimal ways to solve the key problems facing the industry.

Ключові слова: *інформаційна установа, управління, державне регулювання, захист інформації.*

Keywords: *information institution, management, state regulation, information protection.*

Аналіз останніх досліджень. Незважаючи на ту обставину, що питання пов'язані з управлінням діяльністю інформаційних установ досить широко представлені у наукових працях вітчизняних учених, однак особливості їх

управління в умовах воєнного часу розглянуто недостатньо. Окремі питання з досліджуваної проблеми розглянуто у працях З. В. Гбур [4] та Ю. В. Засоки [5].

Постановка наукової проблеми. Враховуючи незначну кількість наукових праць в яких розглянуто питання пов'язані з особливостями управління діяльністю інформаційних установ в умовах воєнного стану, значну роль при висвітленні поставленої проблеми відіграв аналіз нормативно-правових актів. Кардинальні зміни, що відбулися впродовж останнього часу вимагають об'єктивного аналізу державного регулювання управлінських процесів в інформаційній галузі. Протидія інформаційним загрозам з яким постійно зустрічаються інформаційні установи вимагає оптимізації та подальшого вдосконалення управлінських процесів.

Метою статті є дослідження та аналіз змін управлінських процесів в інформаційних установах в умовах воєнного стану, особливостей координації їх діяльності.

Виклад основного матеріалу. Впродовж останніх десятиліть у світі спостерігається процес формування інформаційного суспільства у зв'язку з чим все більше розвиваються інформаційні мережі, що являють собою унікальний симбіоз комунікацій і комп'ютерів. Інформація поступово перетворилася на масовий продукт, потребу в якому відчувають не лише керівники, а й мільйони громадян. У комплексі це пов'язано з децентралізаційними процесами, що відбуваються у суспільстві, підвищенням ступеня свободи індивідів та соціальних груп. Поступово інформація перетворилася з категорії повідомлень в економічну категорію й оцінюється з точки зору ринку і перестала бути безкоштовним товаром. Поступово виник інформаційний ринок на якому інформація стала товаром, операції з яким приносять як прибутки так і збитки [2, с. 6].

Впродовж останніх десятиліть інформація стала основним об'єктом та продуктом нашого суспільства, а комп'ютеризація та інформація, відповідно, головними інструментами її опрацювання. При цьому під інформацією

розуміють сукупність взаємопов'язаних соціально-економічних, політичних, правових та виробничих процесів спрямованих на створення умов для задоволення інформаційних потреб громадян та суспільства за допомогою створення, розвитку і використання «інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки» [1, с. 50-51].

У діяльності сучасних підприємств інформація є неодмінним і головним фактором ефективного функціонування. При цьому, ключове значення набуває забезпечення як оперативності так достовірності відомостей та прийняття правильних рішень на основі інформації. Важливу роль у прийнятті рішень відіграє «науково-технічна інформація, що містить нові наукові знання, відомості про винаходи, технічні новинки підприємства і підприємств-конкурентів» [3]. Це безперервно поповнюваний загальний фонд і потенціал знань і рішень, своєчасне і практичне використання котрого забезпечить установі якісний рівень конкурентоспроможності. У зв'язку з цим, інформація є базою для підготовки відповідних звітів, доповідей, пропозицій спрямованих на вироблення і прийняття управлінських рішень. Зміст інформації визначається потребами певних управлінських ланок і напрацьованих управлінських рішень.

Таким чином, аналізуючи потреби сучасних установ в інформації, для ефективного їхнього функціонування важливо виокремити такі риси прийняття рішень, як цілеспрямована і свідома діяльність, здійснювана керівником; поведінка, заснована на фактах і ціннісних орієнтирах; характер взаємодії членів установи; вибір альтернатив у рамках політичного і соціального стану; частина загального процесу управління тощо [3].

Інформаційні системи управління являють собою певні відомості, дані, оформлені таким чином, щоб забезпечувати зручність прийняття рішень в області певної цільової діяльності. Враховуючи, що потреба в інформації різних суб'єктів і управлінських структур далеко не однакова і визначається, у першу чергу, тими завданнями, що вирішує у процесі управління той або інший, керівник, чи працівник управлінського апарату. Вона також залежить

від таких факторів, як: «масштабу та важливості прийнятих рішень (чим масштабніше та важливіше рішення, тим більша за обсягом та різноманітніша за змістом інформація необхідна для його підготовки та прийняття); кількості та характеру керованих, регульованих параметрів; кількості варіантів можливого стану та поведження керованого об'єкту; величини та розмаїтості внутрішніх і зовнішніх впливів на керовану систему; кількості і якості показників, що характеризують результати функціонування даної системи» [3].

Загалом термін «інформаційна сфера» часто зустрічається у чинному законодавстві, але, на жаль, впродовж значного періоду була відсутня її нормативна дефініція та юридичне закріплення. Межі інформаційної сфери чітко окреслені у статті 3 Закону України «Про інформацію» де відзначено, що дія закону поширюється на інформаційні відносини, що виникають у всіх сферах життєдіяльності держави і суспільства під час одержання, використання та зберігання інформації [9, с. 9-10]. Значно розширене трактування інформаційної сфери знаходиться у Законі України «Про концепцію державної інформаційної політики» в якому вона визначена як «сукупність інформаційних ресурсів, інформаційної інфраструктури, суб'єктів інформаційних відносин, які забезпечують збирання, зберігання, використання та поширення інформації, а також системи правового регулювання суспільних відносин у цій сфері й організації виробництва засобів» [9, с. 10]. Окрім проблеми неоднозначності щодо нормативного визначення, інформаційна сфера характеризується також високим рівнем складності для управління. Активна динаміка розвитку інформаційної сфери не завжди дають змогу державі оперативно реагувати за допомогою управлінських засобів на нові інформаційні явища та процеси. Державне управління інформаційною сферою носить галузевий характер, а такий вид управління, передбачає «здійснення восьми груп функцій:

- організація системи і процесу управління;
- визначення та реалізація політики і стратегії розвитку галузі;
- забезпечення розвитку науково-технічного потенціалу галузі;
- мобілізація та використання ресурсів галузі;

- ситуаційне управління структурами галузі;
- управління розвитком інфраструктури галузі;
- маркетинг і ринок продукції галузі;
- управління інвестиціями, розвитком робочих місць і підготовкою кадрів» [9, с. 10].

При цьому, головну роль відіграє організація системи управління, суб'єктом якого виступає держава як ключовий політичний інститут політичної системи і політичної організації суспільства, який створений для налагодження життєдіяльності суспільства в цілому і здійснення політичної влади у суспільстві з метою забезпечення його цілісності і безпеки, задоволення загально-соціальних проблем. В той же час, управління інформаційною сферою набуває державно-організованих форм, які обумовлені функціями та методами впливу на соціальні відносини. На поверхні державно-правових явищ ці форми проявляються насамперед у структурах державного управління і через ці структури реалізуються [9, с. 10].

Нова стратегія національної безпеки України, яка затверджена Указом Президента України від 14 вересня 2020 р. № 392/2020 визначила поточні та прогнозовані загрози національній безпеці та національним інтересам України, зокрема:

- стрімко зростає роль інформаційних технологій у всіх сферах суспільного життя;
- розробляються системи озброєнь на основі нових фізичних принципів, із використанням квантових, інформаційних, космічних, гіперзвукових, біотехнологій, технологій у сфері штучного інтелекту тощо;
- сучасна модель глобалізації уможливорює поширення міжнародного тероризму та міжнародної злочинності у кіберпросторі;
- поширення коронавірусної хвороби (COVID-19) виявляє критичні проблеми в інформаційній та інших сферах, що загрожує національним інтересам та національній безпеці України [8].

Одним із ключових питань, яке постало перед Україною на сучасному етапі – це вдосконалення системи управління діяльністю інформаційними установами.

Враховуючи ту обставину, що нині в умовах воєнного стану військові дії відбуваються не лише на фронті, а й перенеслися у інформаційний простір, адже розвиток науки та техніки дозволяє це застосовувати. Під інформаційною війною варто розуміти проведення «широкомасштабних інформаційних дій, що застосовуються сторонами» та спрямованих проти соціальних і інформаційно-технічних систем «держави з метою одержання інформаційної переваги над противником» [8, с. 273].

Аналізуючи дане питання доцільним є визначити поділ інформаційної безпеки на її різновиди: людини, держави та суспільства. Зокрема, у Законі України «Про основи національної безпеки України» об'єктами національної безпеки визначено: суспільство та його духовні, культурні, морально-етичні, інтелектуальні цінності, інформаційне і навколишнє природне середовище і природні ресурси, людина та громадянин і їхні конституційні права та свободи, держава та її суверенітет, конституційний лад територіальна цілісність і недоторканність [6, с.109].

Таким чином, здійснюючи керівництво інформаційною установою в умовах загроз та викликів воєнного часу ключову роль необхідно приділяти захисту інформації та посилювати інформаційну безпеку, що позитивно вплине не лише на її діяльність, а й сприятиме захисту інтересів держави.

Відповідно, головним критерієм класифікації інформаційної безпеки необхідно визначити її об'єкти. За цим критерієм відповідно до законодавства виділяють: інформаційна безпека держави, інформаційна безпека людини, інформаційна безпека суспільства [6, с.110].

Серед ключових пріоритетів державної політики у галузі інформаційної безпеки виокремлюють захист важливих інформаційних потреб та інтересів держави, особистості та суспільства. Враховуючи нинішні загрози національній безпеці України на цьому напрямі мають сконцентруватися керівники

інформаційних установ, органи влади, щоб протидіяти загрозам і викликам, що стоять перед суспільством. Враховуючи застосування інформаційних технологій у військово-політичних цілях у тому числі й агресії. У цьому першочергове значення приділяється розробці та впровадженню дієвих механізмів прогнозування, виявлення та оцінки інформаційних загроз, нейтралізації інформаційно-психологічного впливу населення країни, в тому числі спрямованого на підриг національних цінностей та історичної спадщини [7, с. 275-276].

Варто відзначити, що впродовж останніх років Україна зробила багато щодо регулювання інформаційної безпеки на нормативно-правовому рівні. Так, 28 грудня 2021 р. затвердили Стратегію інформаційної безпеки, головною метою прийняття якої є «посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина» [4].

Ефективність сучасної зброї великою мірою визначається не лише вогневою потужністю, а й ступенем інформаційної забезпеченості. В змісті воєнних дій зростає значимість інформаційно-технічного протистояння. Переваги в ступені інформованості це неодмінна умова перемоги [4].

Ключовими факторами щодо забезпечення ефективної діяльності у сфері «державного управління інформаційною безпекою є:

- розробка показників оцінки ефективності систем захисту інформаційної безпеки держави;
- моніторинг та ідентифікація появи дестабілізуючих факторів та загроз;
- організація проведення фундаментальних та прикладних наукових досліджень в галузі забезпечення інформаційної безпеки;
- розробка відповідної нормативно-правової бази;
- протистояння загрози інформаційної війни» [4].

Інформаційна безпека є важливою функцією держави, повинна передбачати, насамперед, формування відповідними державними органами політики організаційно-правових механізмів в галузі інформації [4].

Отже, як бачимо впродовж останніх років в Україні зроблено значні кроки щодо вдосконалення системи управління діяльністю інформаційних установ та здійснено комплекс заходів щодо посилення безпеки інформаційних установ.

Незважаючи на здійснені кроки, які активізувалися після початку ведення воєнних дій в Україні є низка проблем, вирішення має бути здійснено органами влади у першу чергу.

Оскільки новітні технології стали невід'ємною частиною нашого життя, ворожі атаки ставлять під загрозу життя та благополуччя найбільш вразливої частини населення. Основні проблеми, щодо забезпечення безпеки інформаційної об'єктів критичної інфраструктури нашої держави можна узагальнити наступними блоками:

- неефективне (застаріле) нормативно-правове забезпечення процесу кібербезпеки країни;
- неефективна система реагування на кіберінциденти (технологічне відставання, нестача кваліфікованих кадрів, децентралізація управління);
- слабка взаємодія державних та недержавних суб'єктів у процесі забезпечення кібербезпеки держави;
- слабка система кіберрозвідки;
- застаріла система стандартизації у сфері кібербезпеки».

Критична інфраструктура та базові інформаційні послуги, що надає держава стають дедалі більше взаємозалежними та цифровими. Усі підключені до Інтернету пристрої будь то автоматизовані машини, системи промислового управління чи побутова техніка, та цілі ланцюжки поставок, які роблять їх доступними, мають бути захищеними, стійкими до кібератак швидко відновлюватися у випадку виявлення вразливих місць. Це є ключовим для

надання приватному та державному сектору України «можливості вибору з найбільш безпечних інфраструктур та послуг» [5, с 268-269].

Таким чином, як бачимо станом на сьогодні незважаючи на прийняття низки ключових нормативно-правових актів система державного управління інформаційними установами в Україні потребує вдосконалення. Насамперед це стосується покращення системи безпеки їх діяльності, що можливе у результаті налагодження тісної співпраці між приватними й державними структурами, посиленню протидії ворожим атакам.

Література

1. Біленчук П. Д., Кофанов А. В., Кобилянський О. Л. Міщенко В. Б. Інформаційне суспільство: управління, право, технології, безпека. К. 2009. С. 50-51.
2. Білоус Л. І. Управління та організація діяльності інформаційних установ. Навчальний посібник. Тернопіль, 2010. 414 с.
3. Бугас Н. В., Коваленко О. О. Інформаційна система як умова ефективних управлінських рішень. Ефективна економіка. 2016. № 12. [Режим доступу]. <http://www.economy.nayka.com.ua/?op=1&z=5313>
4. Гбур З. В. Основи інформаційної безпеки держави в умовах війни. Електронний ресурс. [Режим доступу]. <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/237/6325/13361-1?inline=1>
5. Заскока Ю. В. Проблеми забезпечення кібербезпеки об'єктів критичної інфраструктури України. Актуальні проблеми управління інформаційною безпекою держави. Збірник тез наукових доповідей. XII Всеукраїнська науково-практична конференція. К. 2021. С. 267-269.
6. Золотар О. О. Класифікація інформаційної безпеки. Інформація і право. 2011. № 2. С. 109-113.
7. Канарський В. С. Пріоритети державної політики інформаційної безпеки України. Актуальні проблеми управління інформаційною безпекою

держави. Збірник тез наукових доповідей. XII Всеукраїнська науково-практична конференція. К. 2021. С. 275-277.

8. Ісайко Д. І Інформаційна війна. Актуальні проблеми управління інформаційною безпекою держави. Збірник тез наукових доповідей. XII Всеукраїнська науково-практична конференція. К. 2021. С. 273-275.

9. Яременко О. Державне управління інформаційною сферою в Україні: структурно-функціональний аспект. Правова інформатика. 2008. № 2. С. 9-17.

References

1. Bilenchuk, P. D., Kofanov, A. V., Kobylanskyi, O. L. and Mishchenko, V. B. (2009), *Informatsijne suspil'stvo: upravlinnia, pravo, tekhnolohii, bezpeka* [Information society: management, law, technology, security], Kyiv, Ukraine, pp. 50-51.

2. Bilous, L. I. (2010), *Upravlinnia ta orhanizatsiia diial'nosti informatsijnykh ustanov* [Management and organization of activities of information institutions], Ternopil, Ukraine.

3. Buhas, N. V. and Kovalenko, O. O. (2016), “Information system as a condition for effective management decisions”, *Efektivna ekonomika*. vol. 12, available at: <http://www.economy.nayka.com.ua/?op=1&z=5313> (Accessed 30 Nov 2022).

4. Hbur, Z. V. (2022), “Basics of information security of the state in conditions of war”, available at: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/237/6325/13361-1?inline=1> (Accessed 30 Nov 2022).

5. Zaskoka, Yu. V. (2021), “Problems of ensuring cyber security of critical infrastructure objects of Ukraine”, *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy. Zbirnyk tez naukovykh dopovidei. XII Vseukrainska naukovo-praktychna konferentsiia*. [Actual problems of state information security management. A collection of theses of scientific reports. XII All-Ukrainian scientific and practical conference], Kyiv, Ukraine, pp. 267-269.

6. Zolotar, O. O. (2011), “Classification of information security”, *Informatsiia i pravo*, vol. 2, pp. 109-113.

7. Kanarskyi, V. S. (2021), “Priorities of the state information security policy of Ukraine”, *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy. Zbirnyk tez naukovykh dopovidei. XII Vseukrainska naukovo-praktychna konferentsiia*. [Actual problems of state information security management. A collection of theses of scientific reports. XII All-Ukrainian scientific and practical conference], Kyiv, Ukraine, pp. 275-277.

8. Isaiko, D. I (2021), “Information war”, *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy. Zbirnyk tez naukovykh dopovidei. XII Vseukrainska naukovo-praktychna konferentsiia*. [Actual problems of state information security management. A collection of theses of scientific reports. XII All-Ukrainian scientific and practical conference], Kyiv, Ukraine, pp. 273-275.

9. Yaremenko, O. (2008), “State management of the information sphere in Ukraine: structural and functional aspect”, *Pravova informatyka*, vol. 2, pp. 9-17.

Стаття надійшла до редакції 10.12.2022 р.