

В. В. Кушніков,
аспірант, Національний аерокосмічний університет
"Харківський авіаційний інститут"
ORCID ID: <https://orcid.org/0009-0003-0843-4516>

DOI: 10.32702/2306-6814.2025.15.311

МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: РОЛЬ ТА СПЕЦИФІКА ФОРМУВАННЯ

V. Kushnikov,
PhD student, National Aerospace University "Kharkiv Aviation Institute"

MECHANISMS OF PUBLIC ADMINISTRATION IN THE FIELD OF INFORMATION SECURITY:
ROLE AND SPECIFICS OF FORMATION

У статті виокремлено роль та специфіку формування механізмів публічного управління у сфері інформаційної безпеки. Зокрема, виділено підсистеми політичної системи як підґрунтя для формування механізмів у сфері інформаційної безпеки. Охарактеризовано переваги цифровізації публічного управління, як одного із перспективних напрямків розвитку механізмів публічного управління у сфері інформаційної безпеки.

Показано, що політична система, як підґрунтя формування механізмів публічного управління у сфері інформаційної безпеки, складається з наступних підсистем: інституційна підсистема — включає державу, громадські об'єднання (громадські організації, зокрема політичні партії передусім) і відносини з-поміж них, які у сукупності утворюють політичну організацію суспільства; комунікативна підсистема — включає в себе всі форми політичної взаємодії як усередині системи, і з політичними системами інших держав; нормативна підсистема — включає в себе політичні, правові, моральні цінності, традиції, звичаї; власне функціональна підсистема — включає способи здійснення влади, методи політичної діяльності.

Акцентовано увагу на розвитку Єдиних центрів обробки інформації необхідні для того, щоб держава мала статистику звернень населення з тих чи інших питань, приймати рішення та робити висновки про те, які проблеми хвилюють населення в першу чергу. Це дозволить виявити на ранній стадії ознаки невдоволення громадян та оперативно на них реагувати, не доводячи ситуацію до масових акцій протесту та інших активних дій, наприклад, вимоги відправити у відставку місцевих керівників.

Запропоновано альтернативні механізми публічного управління у сфері інформаційної безпеки: короткострокове прогнозування розвитку найважливіших процесів у соціально-економічній та фінансовій сфері; оцінка ефективності та повноти реалізації законів та інших нормативно-правових актів із соціально-економічних та фінансових проблем; оцінка ефективності методів, організаційних структур та процесів управління стосовно органів державної влади та місцевого самоврядування, підприємств та організацій усіх форм власності та сфер діяльності.

The article identifies the role and specifics of the formation of mechanisms of public administration in the field of information security. In particular, the subsystems of the political system are allocated as the basis for the formation of mechanisms in the field of information security. The advantages of digitalization of public administration as one of the promising directions of development of mechanisms of public administration in the field of information security are characterized.

It is shown that the political system, as the basis for the formation of mechanisms of public administration in the field of information security, consists of the following subsystems: institutional subsystem — includes the state, public associations (public organizations, in particular political parties above all) and relations among them, which together form the political organization of society; communicative subsystem — includes all forms of political interaction both within the system and with political systems of other states; normative subsystem — includes political, legal and moral values, traditions, customs; the functional subsystem itself — includes methods of exercising of power, methods of political activity.

Attention is focused on the development of Unified Information Processing Centers necessary for the state to have statistics of population appeals on certain issues, to make decisions and draw conclusions about what problems concern the population in the first place. This will make it possible to identify at an early stage signs of dissatisfaction of citizens and quickly respond to them, without bringing the situation to mass protests and other active actions, for example, demands to dismiss local leaders.

The alternative mechanisms of public administration in the field of information security are proposed: short-term forecasting of the development of the most important processes in the socio-economic and financial spheres; assessment of the effectiveness and completeness of the implementation of laws and other normative legal acts on socio-economic and financial problems; assessment of the effectiveness of methods, organizational structures and the processes of management in relation to state authorities and local self-government, enterprises and organizations of all forms of ownership and spheres of activity.

*Ключові слова: публічне управління, інформаційна безпека, органи державної влади, місцеве самоврядування.
Key words public administration, information security, public authorities, local government.*

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Реалізація державної політики забезпечення інформаційної безпеки є просто необхідною для будь-якої демократичної держави, тому що максимальна відкритість для громадян — це один із принципів демократії. Звісно, не потрібно розкривати всі видаткові статті бюджету (наприклад, військові), але пояснити громадянам, куди і на які цілі витрачаються гроші платників податків — прямий обов'язок держави. У цьому зв'язку необхідно вирішити, як саме державі та іншим політичним інститутам, насамперед політичним партіям, найефективніше проводити свою інформаційну політику. Особлива відповідальність лежить, природно, на органах державної влади тих чи інших країн, які здійснюють інформаційну політику або тільки починають її формувати та реалізовувати. Вищезазначене обумовлює актуальність обраної теми дослідження.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Питання дослідження інформаційної безпеки в державі неодноразово підлягали дослідженню з боку ба-

гатьох вчених і практиків, зокрема, таких, як: Т. Амро, А. Ключко, Т. Семенець-Орлова, І. Сердюк та ін. Зокрема, розглядався державно-управлінський аспект інформаційної безпеки, особливості формування та реалізації інформаційної політики держави, специфіка публічного управління інформаційною безпекою особистості та ін. Проте недостатньо уваги приділяється механізмам публічного управління у сфері інформаційної безпеки.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою роботи є виокремлення ролі та специфіки формування механізмів публічного управління у сфері інформаційної безпеки.

Для досягнення поставленої мети в роботі пропонується поставити та вирішити такі завдання:

— виділити підсистеми політичної системи як підґрунтя для формування механізмів у сфері інформаційної безпеки;

— охарактеризувати переваги цифровізації публічного управління, як одного із перспективних напрямків розвитку механізмів публічного управління у сфері інформаційної безпеки;

— запропонувати альтернативні механізми публічного управління у сфері інформаційної безпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Держава займає центральне місце в політичній системі, що являє собою сукупність взаємодіючих між собою норм, ідей та заснованих на них політичних інститутів, установ та дій, що організують політичну владу, взаємозв'язок громадян та держави.

Політична система, як підґрунтя формування механізмів публічного управління у сфері інформаційної безпеки, складається з кількох підсистем, які взаємопов'язані між собою та забезпечують функціонування публічної влади. За функціональною ознакою можна виділити такі підсистеми:

1) інституційна підсистема — включає державу, громадські об'єднання (громадські організації, зокрема політичні партії передусім) і відносини з-поміж них, які у сукупності утворюють політичну організацію суспільства;

2) комунікативна підсистема — включає в себе всі форми політичної взаємодії як усередині системи, і з політичними системами інших держав;

3) нормативна підсистема — включає в себе політичні, правові, моральні і цінності, традиції, звичаї;

4) власне функціональна підсистема — включає способи здійснення влади, методи політичної діяльності [1; 4].

Існує й інша класифікація компонентів політичної системи суспільства:

1) власне політична організація суспільства, що включає державу, політичні партії, інші громадські організації та об'єднання;

2) політична практика, що складається з політичної діяльності та сукупного політичного досвіду;

3) соціально-політичні та правові норми, що регулюють політичне життя суспільства та процес здійснення політичної влади [1; 5].

Як можна побачити, кожен із зазначених варіантів як обов'язковий компонент політичної системи суспільства містить інституційну підсистему.

Будь-яка система передбачає наявність структури, інституційної інфраструктури, на основі якої взаємодіють її різні складові. Понад те, структура постає як основний компонент системи, виконує у ній роль, що поєднує всі елементи системи компонента. Саму структуру політичної системи можна умовно визначити як постійну величину, зміна якої може призвести до серйозних наслідків, а елементи, що складають систему, правильніше розглядати як змінні величини. Звичайно, не варто забувати про те, що політичні системи бувають різні, і інститути характерні для однієї політичної системи, в іншій можуть бути просто відсутніми [2; 3].

Стрижневим елементом політичної системи є держава, оскільки саме вона має монополію на законне насильство та встановлює "правила гри" для решти учасників політичної системи. Справа в тому, що конституція держави і взагалі все чинне законодавство є обов'язковими для виконання абсолютно всіма суб'єктами політичної системи суспільства. У самій державі, відповідно до функціонального поділу влади, діють виконавчі (уряд, міністерства, агентства, служби та ін.), законодавчі (парламент) та судові органи влади. Специфічну

функцію тут виконує адміністративний апарат, який використовується владою як у демократичних, так і в авторитарних державах цілях для вирішення різних завдань. Наприклад, під час передвиборчих кампаній часто можна чути звинувачення з боку опозиції, що кандидатом, близьким до влади, був використаний адміністративний ресурс, тобто допомога з боку місцевих чиновників [1; 2].

Демократія передбачає повну відкритість для громадян, а органи влади у демократичній державі мають бути відкритими — це аксіома. Відповідно, прагнення максимальної відкритості для громадян є природним, і фінансування програм щодо покращення інформаційної складової діяльності державних структур має бути пріоритетним. Ймовірно, це покращить діяльність державних структур, оскільки людям не треба буде приходити до чиновників і запитувати, як заповнювати той чи інший папір, а громадяни легко зможуть ознайомитися з інформацією, що їх цікавить, на сайті даної державної структури.

Одним з важливих моментів є проблема зниження корумпованості державних службовців, і ця проблема актуальна не тільки для України, але і для багатьох розвинених країн, які також схильні до корупції. Тому необхідно зробити мінімальною необхідність спілкування між адміністративними структурами та громадянами. Вирішення проблеми корумпованості можливе у разі збільшення витрат на інформаційну політику державних структур та створення таких умов, коли громадянин буде в курсі: що і як йому робити без допомоги державного службовця, а через інформацію, отриману на сайті цієї організації [3; 5].

Говорячи про поліпшення роботи державних структур та цифровізації публічного управління, як про один із перспективних напрямків розвитку механізмів публічного управління у сфері інформаційної безпеки, не можна забувати про комп'ютеризацію робочих місць державних службовців та необхідність залучення фінансування програм щодо розповсюдження єдиних центрів обробки запитів громадян. Єдині центри обробки інформації необхідні для того, щоб держава мала статистику звернень населення з тих чи інших питань, приймати рішення та робити висновки про те, які проблеми хвилюють населення в першу чергу. Це дозволить виявити на ранній стадії ознаки невдоволення громадян та оперативно на них реагувати, не доводячи ситуацію до масових акцій протесту та інших активних дій, наприклад, вимоги відправити у відставку місцевих керівників.

Ефективним може лише той інформаційний центр, у якому інформація регулярно оновлюється, обробка даних здійснюється у безупинному режимі. Не можна допустити, щоб інформація застаріла. А це означає, що інформаційні масиви потрібно утримувати в оновлюваному режимі і регулярно вносити до них всі зміни та доповнення, бо це має велике значення для ефективної дії системи [1; 3].

Своєчасне виявлення змін, що відбуваються в соціально-економічній та фінансовій сфері держави та регіонів, та причин, що їх викликали, попередження негативних тенденцій, що ведуть до формування та розвитку вогнищ напруженості у соціально-економічній та фінансовій сфері допоможуть зробити державну політику за-

безпечення інформаційної безпеки дієюю [4; 6]. У цьому зв'язку необхідно виокремити відповідні механізми публічного управління у сфері інформаційної безпеки:

— короткострокове прогнозування розвитку найважливіших процесів у соціально-економічній та фінансовій сфері;

— оцінка ефективності та повноти реалізації законів та інших нормативно-правових актів із соціально-економічних та фінансових проблем;

— оцінка ефективності методів, організаційних структур та процесів управління стосовно органів державної влади та місцевого самоврядування, підприємств та організацій усіх форм власності а сфер діяльності.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Таким чином, Регулярне здійснення моніторингу дозволить вирішувати проблеми на ранній стадії і, можливо, навіть зберігати стабільність у регіонах та на загальнодержавному рівні, природно, при оперативній реакції чинної влади як на місцях, так і у вищих органах влади. Державі та державним структурам краще дізнаватися про проблеми регіону за допомогою моніторингу та ретельного аналізу. Крім того, необхідно, щоб люди дізнавалися про проблеми від самого уряду, ніж із повідомлень преси. Саме ці механізми дозволять зробити державну політику забезпечення інформаційної безпеки максимально результативною.

Література:

1. Панченко О. А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект. Київ: КВІЦ, 2020. 331 с.

2. Савоско Т. Особливості формування державної інформаційної політики. Аспекти публічного управління. 2024. № 12 (1). С. 22—28.

3. Ситник Г. П., Клименко Н. Г., Гореліков І. О. Державна політика забезпечення інформаційної безпеки та кібербезпеки, як її складової: проблеми та шляхи їх вирішення. Державне управління: удосконалення та розвиток. 2024. № 5. URL: http://nbuv.gov.ua/UJRN/Duur_2024_5_6.

4. Семенець-Орлова І., Ключко А., Амро Т. Публічне управління у сфері інформаційної безпеки для забезпечення розвитку демократії в Україні (контекст воєнного стану). Публічне урядування. 2024. № 5 (33). С. 73—82.

5. Сердюк І. А. Підходи публічного управління до інформаційної безпеки особистості. Публічне урядування. 2022. № 3 (31). С. 53—59.

6. Сілаєв В., Горінов П. Політика інформаційної безпеки в умовах цифрової трансформації України: виклики та шляхи попередження. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 2024. № 3 (75). С. 81—87.

References:

1. Panchenko, O. A. (2020), Informatsiina bezpeka v epokhu turbulentnosti: derzhavno-upravlinskiy aspekt [Information security in the era of turbulence: the state-management aspect], KVITs, Kyiv, Ukraine.

2. Savosko, T. (2024), "Features of the formation of state information policy", Aspekty publichnoho upravlinnia, vol. 12 (1), pp. 22—28.

3. Semenets-Orlova, I., Klochko, A. and Amro, T. (2024), "Public administration in the field of information security to ensure the development of democracy in Ukraine (the context of martial law)", Publichne uriaduvannia, vol. 5 (33), pp. 73—82.

4. Serdiuk, I. A. (2022), "Public administration approaches to information security of the individual", Publichne uriaduvannia, vol. 3 (31), pp. 53—59.

5. Silaiev, V. and Horinov, P. (2024), "Information security policy in the context of digital transformation of Ukraine: challenges and ways of prevention", Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia, vol. 3 (75), pp. 81—87.

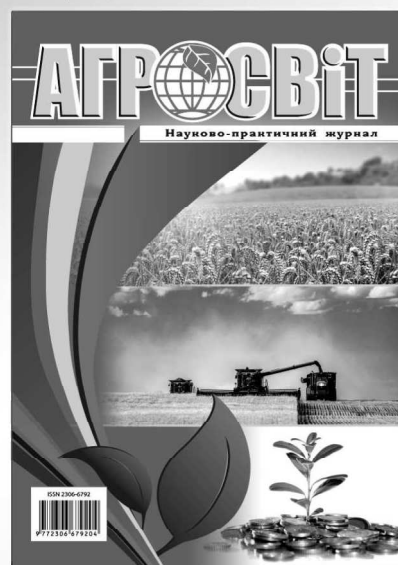
6. Sytnyk, H. P., Klymenko, N. H. and Horielikov, I. O. (2024), "State policy of ensuring of information security and cybersecurity as its component: problems and ways to solve", Derzhavne upravlinnia: udoskonalennia ta rozvytok, vol. 5. http://nbuv.gov.ua/UJRN/Duur_2024_5_6.

Стаття надійшла до редакції 12.07.2025 р.

АГРОСВІТ

<https://nayka.com.ua>

Передплатний індекс: 23847



Виходить 24 рази на рік

Журнал включено до переліку наукових фахових видань України з ЕКОНОМІЧНИХ НАУК (Категорія «Б»)

Спеціальності – 051, 071, 072, 073, 075, 076, 292