ОСОБЛИВОСТІ РОЗУМІННЯ ФЕНОМЕНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ

FEATURES OF UNDERSTANDING THE PHENOMENON OF INFORMATION SECURITY IN THE SPHERE OF PUBLIC ADMINISTRATION

УДК 342.5:327
DOI https://doi.org/10.32782/pma2663-5240-2023.34.21

Дрига Д.А.,
аспірант, Відкритий міжнародний університет розвитку людини

Статтю присвячено дослідженню особливостей розуміння феномену інформаційної безпеки в сучасному публічному управлінні. В ході дослідження основну увагу акцентовано на аналізі та узагальненні підходів вітчизняних дослідників як до самого феномену інформаційної безпеки, так і до її ролі в публічному адмініструванні. З'ясовано, що вітчизняний науковий простір пропонує широку палітру тлумачень інформаційної безпеки. Більшість із них, однак, можна класифікувати на такі групи як: сприйняття інформаційної безпеки як стану стабільності інформаційних систем; сприйняття інформаційної безпеки як гарантії прав і свобод людини щодо користування інформацією; сприйняття інформаційної безпеки як складової національної безпеки. Характерно, що перелічені підходи не є взаємозаперечними, і можуть розглядатися паралельно. Окрему увагу присвячено проблематиці загроз інформаційній безпеці у сучасному світі. Запропоновано ключовою та висхідною загрозою розглядати інформаційний вибух, як процес, що призводить до безконтрольно-хаотичного зростання маси інформації, що несе в собі безліч загроз, не обов'язково є об'єктивною, актуальною, законною і навіть достовірною. Саме інформаційний вибух загострює інші проблеми, такі як розвиток технологій, що впливають на життя людини, її мислення і спілкування, зростання контролю за особистим життям людей та неготовність керівництва держав до реагування на нові інформаційні загрози. Зазначено, що високі темпи впровадження електронного урядування несуть в собі не лише численні переваги, але й велику кількість інформаційних загроз. На прикладі проєкту «Дія» продемонстровано вразливість таких систем до зовнішнього впливу. Подальшої уваги заслуговують тенденції ширшого впровадження технологій штучного інтелекту, що неодмінно набуватиме розвитку і нестиме в собі як нові можливості так і нові загрози.

Ключові слова: *безпека, інформація, інформаційна безпека, національна безпека, публічне адміністрування, суб'єкти публічного адміністрування, інформаційні загрози, джерела інформаційних загроз, електронне урядування.*

The article is devoted to the study of the peculiarities of understanding the phenomenon of information security in modern public administration. In the course of the research, the main focus is on the analysis and generalization of the approaches of domestic researchers both to the phenomenon of information security itself and to its role in public administration. It was found that the domestic scientific space offers a wide range of interpretations of information security. Most of them, however, can be classified into such groups as: perception of information security as a state of stability of information systems; perception of information security as a guarantee of human rights and freedoms regarding the use of information; perception of information security as a component of national security. It is characteristic that the listed approaches are not mutually exclusive and can be considered in parallel. Particular attention is devoted to the problem of threats to information security in the modern world. It is proposed to consider the information explosion as a key and rising threat, as a process that leads to the uncontrolled and chaotic growth of the mass of information, which carries many threats, is not necessarily objective, relevant, legal and even reliable. It is the information explosion that exacerbates other problems, such as the development of technologies that affect people's lives, their thinking and communication, the growth of control over people's personal lives, and the unpreparedness of state leaders to respond to new information threats. It is noted that the high rate of implementation of electronic governance carries not only numerous advantages, but also a large number of informational threats. The vulnerability of such systems to external influence is demonstrated on the example of the "Diia" project. The trends of wider implementation of artificial intelligence technologies deserve further attention, which will certainly develop and bring both new opportunities and new threats.

Key words: *security, information, informational security, National security, public administration, subjects of public administration, information threats, sources of information threats, electronic government.*

Постановка проблеми у загальному вигляді. Проблема безпеки, в сучасному світі, лишається однією з ключових викликів, що постають як перед окремими громадянами, так і перед державами і навіть їх блоками. І найчастіше, увагу привертає саме проблема інформаційної безпеки, адже інтенсивність процесів збирання, обміну, зберігання інформації зростає невпинно, а отже – зростають і ризики та загрози, які вона тягне за собою.

Тотальне проникнення інформаційних технологій, без яких складно собі уявити бодай день життя сучасного українця, було б вражаючим для наших громадян ще якихось 20-30 років тому. Натомість, щоденно кожен з нас використовує мегабайти та гігабайти інформаційного контенту, який формує наші уявлення про життєві цінності, державу, суспільство і наше в ньому місце. І увесь цей потік інформації сповнений загроз, які можуть переходити межі особистого інфопростору, вимагаючи реагування з боку держави, а отже – належного публічного адміністрування проблематикою протидії інформаційним загрозам. Зазначене

й обумовлює актуальність дослідження особливостей розуміння феномену інформаційної безпеки в публічному управлінні.

Аналіз останніх досліджень і публікацій. Основоположні засади публічного управління в контексті національної та інформаційної безпеки вивчали численні вітчизняні та зарубіжні науковці, зокрема: О. Ю. Амелін, І. В. Арістова, С. С. Бучик, О. І. Варченко, В. І. Григор'єв, Ю. С. Довгаль, Я. М. Жарков, І. Ф. Корж, В. В. Кульчицький, С. О. Лисенко, О. В. Литвиненко, Л. Р. Наливайко, А. Ю. Нашинець-Наумова, О. А. Панченко, В. Г. Пилипчук, А. М. Подоляка, Є. Д. Скулиш, В. Ю. Степанов, В. С. Цимбалюк, Т. С. Яровой та ін.

Виділення невирішених раніше частин загальної проблеми. При цьому, узагальнення їх підходів щодо трактування ними феномену інформаційної безпеки в галузі публічного адміністрування в Україні, у вітчизняній науці зроблено не було, що й обумовлює актуальність нашого дослідження.

Метою статті виступає систематизація вітчизняних наукових напрацювань, які присвячені особливостям розуміння феномену інформаційної безпеки у сфері публічного управління.

Виклад основного матеріалу. Проблематика розуміння інформаційної безпеки як сучасного феномену, сфери публічного адміністрування, вимагає врахування як наукових підходів, так і аналізу практики діяльності державних органів у цій царині. Ще понад 15 років тому видатна вітчизняна дослідниця інформаційного права І. Арістова наголошувала на тому, що головною довгостроковою метою державної інформаційної політики України є формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави, його інтеграція у світовий інформаційний простір з урахуванням національних особливостей і інтересів під час забезпечення інформаційної безпеки на внутрішньодержавному та міжнародному рівнях [1]. І варто зазначити, що це твердження набуло ще більшої актуальності в умовах сучасності.

Наразі у вітчизняному науковому середовищі дефініція «інформаційна безпека» тлумачиться крізь призму різних наукових підходів. На думку В. Горового, це, в першу чергу, відсутність небезпеки, тобто тих чинників та умов, які загрожують безпосередньо індивіду, державі, спільноті з боку інформаційно-комунікаційного середовища. Тобто інформаційна безпека розглядається як стан та процес захищеності особи, суспільства, держави від реальних або потенційних загроз [2, с. 34]. Натомість, С. Горова пропонує розглядати інформаційну безпеку як стан захищеності саме «інформаційного середовища, який відповідає інтересам держави та забезпечує формування, використання і можливості розвитку, незалежно від впливу внутрішніх і зовнішніх інформаційних загроз» [3, с. 101]. Тобто за такого підходу інформаційна безпека тлумачиться крізь призму «стану захищеності» того чи іншого об'єкта (особи, суспільства, держави, інформаційного середовища).

В. Лужецький та О. Войнович тлумачать інформаційну безпеку як стан інформаційного середовища суспільства і політичної еліти, що забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства [4, с. 128]. О. Тихомиров – як стан захищеності інформації, яка забезпечує життєво важливі інтереси людини [5]. Такі визначення видаються аж надто узагальненими, оскільки відповідають тлумаченню якостей, функцій чи гарантій інформаційної безпеки, а не її самої.

Та найбільш комплексним видається тлумачення Б. Кормича, який розглядає інформаційну безпеку як інформаційний компонент національної безпеки по співвідношенню «частина-ціле», характеризуючи національну безпеку як стан захищеності держави від внутрішніх і зовнішніх загроз, що забезпечує умови існування людини, держави і суспільства, які гарантовані Конституцією та законами України [6, с. 132]. Характерно, що такий підхід корелюється з чинним законодавством, до чого ще повернемося згодом.

В цілому ж, інформаційну безпеку, в контексті публічного адміністрування, доцільно розглядати як складову національної безпеки, що реалізує стан захищеності людини і громадянина, суспільства і держави, від загроз інформаційного характеру. Саме інформаційна безпека є запорукою стабільного збору, обробки, передачі та отримання, зберігання та видалення інформації будь-якого характеру на будь-яких носіях.

За такого підходу, інформаційна безпека є без перебільшення мультидисциплінарним явищем та складною галуззю суспільних відносин. Її підтримка вимагає використання напрацювань у таких галузях як математика, фізика, хімія, біологія, філософія, психологія, логістика, право, державне управління, економіка, соціологія тощо. Оскільки кожен вид діяльності в сучасному світі так чи інакше просякнутий інформаційними процесами – інформаційна безпека виступає невід'ємною складовою безпеки у найширшому її сенсі.

Окремі дослідники (О. Панченко, В. Антонов, А. Малєєва) навіть акцентують увагу на такому

прояві інформаційної безпеки як інформаційно-психологічна безпека. Розглядаючи її як «забезпечення психологічного благополуччя особистості з мінімізацією різноманітних ризикових факторів формування й функціонування адекватної інформаційно-орієнтовної основи суб'єктивно-особистісних відносин до навколишнього світу й самої себе» [7]. І у вітчизняній і у світовій науці є й інші численні варіанти бачення проявів інформаційної безпеки.

Не дивно, що важливість інформаційної безпеки не лишилася і осторонь уваги правотворців. Відповідно до Закону України «Про національну безпеку» (п 4. ст. 3): «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями» [8]. Окрім того, статтею 19 згаданого Закону, питання інформаційної безпеки покладено, в першу чергу, на Службу безпеки України. Адже саме до її компетенції законодавець відносить: «…контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, інформаційної безпеки держави, об'єктів критичної інфраструктури» [8]. Звісно, чималу ролі у реалізації інформаційної безпеки на національному рівні відіграють і інші служби й відомства (наприклад – Державна служба спеціального зв'язку та захисту інформації України). Однак, саме наукова спільнота, як і в ряді інших галузей, перебуває на передньому краї розвідки проблематики, окреслюючи основні перспективи та загрози інформаційній безпеці у галузі публічного управління.

Доволі цікавий аналіз загроз інформаційній безпеці наводить у своїх працях Т. Ткачук. На переконання дослідника, ключовими загрозами інформаційній безпеці в Україні можна вважати: процес інформаційного вибуху; бурхливий розвиток технічних засобів; поширення електронного контролю за життям людей; відсталість управлінської інфраструктури [9].

Спробуємо розглянути пропонований перелік детальніше. Процес інформаційного вибуху почав розглядатися у другій половині XIX століття. Своєрідним популяризатором цього визначення став відомий письменник-фантаст С. Лем. Однак, вже у 2003 році каліфорнійські дослідники довели його наукову спроможність. Цивілізаційні тренди розвитку інформаційного суспільства характеризуються тим, що в одному лише 2002 році людством було створено 18 Ексабайт інформації. При цьому, з 1998 по 2002 рік людство виробило більше інформації більше, ніж за всю попередню історію [10]. З того часу темпи продукування інформації лише зростали. Але разом із корисною та необхідною для розвитку суспільства інформацією, інформаційний простір заповнив необ'єктивний, шкідливий, а часто злочинно-небезпечний контент, яка негативно впливає на спосіб мислення, культуру, рівень управління системи державного управління, моральні засади суспільства, що ставлять під сумнів саму державність, суверенітет і територіальну цілісність [9]. Таким чином, процес інформаційного вибуху однозначно заслуговує на перше місце у рейтингу джерел інформаційних загроз. Окрім того, більшість інших загроз так чи інакше пов'язана саме з цим процесом.

Активний розвиток спеціальних технічних засобів нового класу, які здатних впливати як на психіку і свідомість людей, так і на інформаційно-технічну інфраструктуру, спостерігається останніми роками і стає помітним навіть не фахівцям. До цієї ж категорії загроз можна віднести поширення електронного контролю за життям, настроями, планами громадян, політичних організацій тощо [9]. При цьому, варто зважати, що у більшості випадків люди самі необдумано дозволяють відслідковувати інформаційні потоки, підтверджують таргетування реклами, дають доступ до місця свого знаходження тощо.

Своєрідною реакцією на загрози і водночас їх наслідком є відверто відстаючі темпи розвитку інформаційної управлінської інфраструктури. У більшості випадків керівництво схильне недооцінювати інформаційні загрози, а обговорення цієї теми в публічному просторі взагалі таврується як параноя, і відверто висміюється, що в умовах демократичного суспільства не може спряти просуванню до високих адміністративних посад осіб, які проявляють обачність і озвучують свої думки щодо інформаційних загроз та тенденцій їх поширення.

Окрему увагу наукової спільноти, як і суспільства в цілому, привертає дедалі більша цифровізації державних послуг, зокрема – проєкт «Дія». Міністерство цифрової трансформації України за два роки існування проєкту додало до нього чимало корисних функцій (таких як електронні документи, можливість отримання довідок з податкової служби, електронний сертифікат про вакцинацію від COVID-19 тощо) [11]. При цьому, система неодноразово зазначала збоїв з технічних причин [12; 13]. Хоча існують цілком обґрунтовані побоювання і щодо можливостей витоку інформації

з системи внаслідок хакерських атак [14], що набуває особливої гостроти в умовах війни.

Висновки. Узагальнення поширених у вітчизняному науковому середовищі підходів до інформаційної безпеки в контексті публічного управління, дає підстави стверджувати про значну розробленість даної тематики, яка, однак, актуалізується високими темпами розвитку інформаційних технологій та відповідно – високою динамікою появи нових інформаційних загроз.

Інформаційну безпеку, в контексті публічного адміністрування, доцільно розглядати як складову національної безпеки, що реалізує стан захищеності людини і громадянина, суспільства і держави, від загроз інформаційного характеру. Саме інформаційна безпека є запорукою стабільного збору, обробки, передачі та отримання, зберігання та видалення інформації будь-якого характеру на будь-яких носіях.

Вітчизняні дослідники вже не перший рік вивчають такі складові інформаційної безпеки як кібербезпека, інформаційно-психологічна безпека тощо. При цьому, вони тільки починають розглядати сучасні феномени інформаційного суспільства, такі як соціальні мережі, месенджери.

Особливої гостроти проблематика інформаційної безпеки крізь призму публічного управління набуває з огляду на розробку і впровадження таких проєктів як «Дія». Неодноразові збої технічного забезпечення якої вже були наявні, хоча поки й не призвели до серйозних наслідків.

Окремої уваги дослідників, у контексті інформаційної безпеки у публічному управлінні заслуговує дедалі ширше впровадження технологій штучного інтелекту, що неодмінно набуватиме розвитку і нестиме в собі як нові можливості так і нові загрози.

ЛІТЕРАТУРА:

1. Арістова, І. В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія. Харків: Нац. ун-т внутр. справ, 2006. 354 с.

2. Горовий В. Формування стратегічного наративу інформаційного забезпечення реінтеграції тимчасово окупованих територій у загальноукраїнський контекст / В. Горовий, О. Онищенко, Ю. Половинчак та ін. Київ, 2017. 212 с.

3. Горова С. В. Особа в інформаційному суспільств і: виклики сьогодення / С. В. Горова. Київ, 2017. 452 с.

4. Лужецький В. А. Інформаційна безпека / В. А. Лужецький, О. П. Войнович, А. В. Дудатьєв. Вінниця: УНІВЕРСУМ-Вінниця, 2009. 240 с.

5. Тихомиров О. О. Класифікації забезпечення інформаційної безпеки. URL : http://www.law.journalsofznu.zp.ua/archive/visnik-1-2011/29.pdf.

6. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України / Б. А. Кормич. Одеса: Юридична література, 2003. 314 с.

7. Панченко О. А., Антонов В. Г., Малєєва А. М., Державне управління інформаційною безпекою як запорука особистісного благополуччя. Механізми публічного управління. Вчені записки ТНУ імені В. І. Вернадського. Серія: Державне управління. 2020. Том 31 (70) № 4. С. 81-87.

8. Про національну безпеку: Закон України від 21.06.2018 р. № 2469-VIII. Офіційний веб-портал Верховної Ради України. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text

9. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. Підприємство, господарство і право. 2017. № 10. С. 182-186. URL : http://pgp-journal.kiev.ua/archive/2017/10/38.pdf

10. Lyman P., Varian H.R. How much information. Release of the University of California. Oct.27, 2003.

11. Державні послуги онлайн. URL : https://diia.gov.ua/

12. У "Дії" стався масштабний збій - з додатка зникли майже всі документи. Уніан. 02.11.21. Уніан. Електронний ресурс. Вилучено з URL: https://www.unian.ua/science/u-diji-stavsya-masshtabniy-zbiy-z-dodatka-znikli-mayzhe-vsi-dokumenti-novini-11597242.html

13. У перший день бета-тестування "єПідтримки" у роботі "Дії" стався збій. Що відомо. Ярослав Лепеха. Суспільне новини. 13 грудня 2021. Електронний ресурс. Вилучено з URL: https://suspilne.media/189187-u-dii-v-den-zapusku-epidtrimki-stavsa-zbij-so-vidomo/

14. FEDOROV. Telegram. Feb 15, 2022. Електронний ресурс. Вилучено з URL : https://t.me/zedigital/1056