ISSN 2072–8670 (Print)
НАУКА І ПРАВООХОРОНА
NAUKA I PRAVOOKHORONA
DOI (Issue): https: //doi.org/10.36486/np.2020.2(48) Issue 2(48) 2020

ІНФОРМАЦІЙНЕ ПРАВО. ПРАВО ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

УДК 342.951(477)

Онопрієнко Станіслав Григорович,
кандидат юридичних наук,
старший викладач кафедри правового забезпечення
Військового інституту Київського
національного університету
імені Тараса Шевченка, м. Київ, Україна
ORCID ID 0000-0002-5524-1798

ІНФОРМАЦІЙНА БЕЗПЕКА СФЕРИ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ

Стаття присвячена визначенню сутності інформаційної безпеки сфери публічного адміністрування. Запропоновано визначення публічного адміністрування та публічного інтересу. Аргументовано, що інформаційна безпека сфери публічного адміністрування являє собою складову національної інформаційної безпеки, яку можна представити як сукупність інформаційної безпеки законодавчої і судової влади, а також інформаційної безпеки органів публічного адміністрування. Обґрунтовано, що інформаційна безпека сфери публічного адміністрування може також бути класифікована за характером ризиків.

Ключові слова: *інформаційна безпека, публічне адміністрування, кібербезпека, інформаційні правовідносини, інформаційна культура, ризики, публічне управління, інформаційні технології.*

Проблеми забезпечення інформаційної безпеки надзвичайно загострилися нині, коли процеси публічного адміністрування в нашій державі відчувають значний вплив цифровізації. Цифровий розвиток управлінських технологій, яким би прогресивним він не був, не дозволяє усунути основну небезпеку функціонування будь-яких інформаційно-телекомунікаційних систем, якою є поведінка користувача. Отже, вирішення проблеми зміцнення інформаційної безпеки сфери публічного адміністрування залежить нині не скільки від розвитку інформаційних технологій, скільки від наявності системної комплексної роботи, спрямованої на підвищення рівня інформаційної культури та інформаційної свідомості учасників публічних правовідносин. Вказане обумовлює актуальність дослідження проблем інформаційної безпеки сфери публічного адміністрування.

Слід сказати, що проблеми забезпечення інформаційної безпеки у публічних правовідносинах були предметом наукових досліджень І. Арістової, К. Бєлякова, В. Гавловського, О. Дзьобаня, О. Золотар, Б. Кормича, А. Марущака, В. Цимбалюка та багатьох інших науковців. Разом з тим доводиться констатувати недо-

DOI (Article): https: //doi.org/10.36486/np.2020.2(48).27

статність напрацювань, в яких визначалися б поняття та принципи інформаційної безпеки сфери публічного адміністрування та напрями її забезпечення, що обумовлює спрямованість подальших наукових пошуків.

Метою написання статті є визначення сутності інформаційної безпеки сфери публічного адміністрування.

Категорія "публічне адміністрування" не так давно закріпилося у правовій науці. Сьогодні під ним розуміють "діяльність публічної адміністрації щодо задоволення загальних публічних інтересів соціуму" [1, с. 23], "скоординовані групові дії з питань державних справ" [2, с. 235], "систематично здійснювану діяльність органів державної влади, спрямовану на упорядкування суспільних відносин з метою попередження небезпечних явищ, забезпечення стабільного стану і розвиток суспільних процесів в інтересах оптимального функціонування та розвитку суспільства та держави" [3, с. 71]. Який би підхід до сутності публічного адміністрування – широкий чи вузький – не використовував дослідник, незмінним залишається здійснення вказаного процесу особливими суб'єктами і його спрямованість на задоволення інтересів держави та суспільства. На нашу думку, важливим також є ознака регламентованості дій суб'єктів публічного адміністрування приписами відповідних законодавчих та підзаконних правових актів, за невиконання яких вони несуть юридичну відповідальність, а також підконтрольність суб'єктів публічного адміністрування, що включає можливість здійснення державного, муніципального та громадського контролю за їх діями.

Вказане дає змогу сформулювати наступне поняття: "публічне адміністрування – це визначена законодавчими та підзаконними правовими актами діяльність державних органів, органів місцевого самоврядування та їх посадових осіб, спрямована на задоволення публічних інтересів, яка передбачає настання юридичної відповідальності за порушення правових приписів та здійснення державного, муніципального та громадського контролю".

Поняття інформаційної безпеки також розглядається у багатьох аспектах: як "комплекс нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації і профілактики компютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо" [4], як "одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами" [5, с. 48], як "вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності" [6, с. 48], "захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією України умови існування і розвитку людини, всього суспільства та держави" [7, с. 241]. Розгляд категорії "інформаційна безпека" як вид суспільних відносин, їх елемент або кінцевий

варіант їх реалізації дозволив авторам сформулювати велику кількість класифікацій видів досліджуваного феномену. Найбільш повною та аргументованою нам уявляється позиція О. Золотар, яка за об'єктною ознакою виокремлює такі види інформаційної безпеки: людини; юридичних осіб; суспільства; держави (національна інформаційна безпека); міжнародного співтовариства. Відповідно до загроз інформаційній безпеці авторка пропонує розмежовувати внутрішню і зовнішню інформаційну безпеку, при чому зміст кожної визначається залежно від того, що чи хто є об'єктом інформаційної безпеки [8, с. 112]. Спробуємо знайти місце інформаційної безпеки суб'єктів публічного адміністрування відповідно до наведеної класифікації.

Як ми вже казали вище, відносини, що складаються у сфері публічного адміністрування, спрямовані на забезпечення публічного інтересу. Під публічним інтересом ми розуміємо сукупність цілей, прагнень, потреб, які виникають у фізичних та юридичних осіб у процесі їх діяльності (життєдіяльності), задоволення яких потребує здійснення суб'єктами публічного адміністрування юридично значущих дій. Отже, ті учасники суспільних відносин у сфері публічного адміністрування, які не мають статусу посадових осіб органів державної влади і місцевого самоврядування, можуть бути фізичними особами, представниками громадянського суспільства, суб'єктами господарської діяльності тощо. Для кожного з них реалізація свого публічного інтересу за участю органів публічного адміністрування породжує ситуацію ризику, ситуацію можливого виникнення інформаційної небезпеки. Як приклад можемо навести ситуацію, коли у відкритий доступ потрапили 26 млн посвідчень водія, доступ до яких здійснювався завдяки функціонуванню бота "UA Baza" месенджера Телеграм (причини чого так і залишилися невідомими). Обов'язок представників системи публічного адміністрування забезпечувати безпеку персональних даних, у тому числі тих, які створюються під час надання адміністративних послуг, має, на нашу думку, розглядатися на загальнодержавному рівні інформаційної безпеки. Отже, інформаційна безпека сфери публічного адміністрування, на нашу думку, являє собою складову національної інформаційної безпеки, яку, на наш погляд, можна представити як сукупність інформаційної безпеки законодавчої і судової влади, а також інформаційної безпеки органів публічного адміністрування (як сукупності органів виконавчої влади і органів місцевого самоврядування). При цьому, відповідно до специфіки функціонування органів публічного адміністрування, загрози інформаційній безпеці у їх діяльності можуть мати як зовнішній, так і внутрішній характер.

Інформаційна безпека сфери публічного адміністрування може також бути класифікована за характером ризиків. Якщо ризики мають технологічний характер і стосуються безпеки обладнання та програм, використовують поняття "кібербезпека". У Законі України "Про основні засади забезпечення кібербезпеки України" кібербезпека розуміється як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [9]. Невдалість вказаного легального визначення значним чином утруднює його розуміння,

оскільки більшість його складових потребує окремого тлумачення. Так само було б доцільно для цілісного сприйняття розмежувати категорію "кібербезпека" з категорією "інформаційна безпека". На нашу думку, кібербезпека є складовою інформаційної безпеки, поряд з особистою та корпоративною інформаційною безпекою. Однак обґрунтування вказаної позиції та розробка пропозицій щодо правового закріплення такого розмежування потребують здійснення окремих наукових досліджень.

Окремо слід сказати про чинники, які знижують рівень інформаційної безпеки сфери публічного адміністрування. До них, на нашу думку, належать як зовнішні (інформаційно-психологічні операції, спрямовані на дестабілізацію діяльності органів публічного адміністрування, стан їх технологічної оснащеності), так і внутрішні (існування логічної та зрозумілої для будь-якого суб'єкта інформаційних правовідносин системи вимог щодо забезпечення інформаційної безпеки, а також рівень інформаційної культури як представників органів публічного адміністрування, так громадян, які вступають з ними у правовідносини з метою реалізації своїх інтересів). На особистісному рівні інформаційна культура може бути описана на ціннісно-мотиваційному рівні, який є визначальним для всіх інших складових; когнітивному рівні; який включає у тому числі наявність інформаційних знань, вмінь та навичок; а також на емоційно-вольовому рівні, який обумовлює емоційне відношення до застосування та розвитку вказаних знань, вмінь та навичок, а також прийняття рішень щодо їх застосування в певних ситуаціях [10, с. 136]. На жаль, сучасний рівень інформаційної культури представників сфери публічного адміністрування не можна визнати задовільним. Особливо разючими є відмінності цифрової грамотності залежно від віку та місця проживання персоналу органів публічного адміністрування: особи передпенсійного віку, що мешкають у селах, селищах та невеликих містах, як правило, відчувають значні труднощі під час використання цифрових технологій, що обумовлює одночасне виникнення великої кількості ризиків, пов'язаних з інформаційною безпекою їх діяльності. Одним із способів подолання такої цифрової нерівності мала б стати програма цифрової освіти, яка включала б не лише 5 хвилинні фільми про загальні принципи роботи невеликої кількості окремо узятих інструментів Google (як це реалізовано зараз на платформі "Цифрова грамотність державних службовців 1.0. на базі інструментів Google"), а й передбачало б напрацювання державними службовцями та службовцями органів місцевого самоврядування практичних навичок у сфері інформаційної безпеки. Для забезпечення викривлення результатів такого навчання через вплив корпоративної солідарності і сам процес навчання, і оцінювання його результатів мало б здійснюватися незалежними суб'єктами на принципах аутсорсингу або "запозиченої праці" [11].

Проблеми підвищення рівня інформаційної безпеки сфери публічного адміністрування є надзвичайно важливими у сучасний період реформування системи публічного управління. Вирішення цих проблем потребує використання низки заходів політичного, економічного, технологічного, соціально-психологічного характеру. Проте саме право має стати тією інтегруючою категорією, яка органічно поєднає різновекторні складові інформаційної безпеки, надасть останній

структурований характер, дасть змогу кожному суб'єкту правовідносин у сфері публічного адміністрування розуміти коло своїх прав та обов'язків, а також міру своєї юридичної відповідальності за порушення правових приписів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Кузьменко О.В.* Правова детермінація поняття публічне адміністрування. Повітряне і космічне право. 2009. № 3. С. 20–24.
2. *Лук'янець Д.М.* Форми реалізації державної влади в сучасній Україні. Правова держава: щорічник наукових праць. 2012. Вип. 23. С. 233–239.
3. *Пилипишин В.П.* Адміністративний аспект публічного адміністрування. Наукові записки Інституту законодавства Верховної Ради України. 2015. № 6. С. 68–71.
4. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text (дата звернення: 11.02.2020).
5. *Литвиненко О.* Інформація і безпека. Нова політика. 1998. № 1. С. 47–49.
6. *Фурашев В.М.* Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки. Інформація і право. 2012. № 1(4). С. 46–56.
7. *Кормич Б.А.* Організаційно-правові засади політики інформаційної безпеки України: Монографія. Одеса: Юридична література, 2003. 472 с.
8. *Золотар О.О.* Класифікація інформаційної безпеки. Інформація і право. 2011. № 2. С. 109–113.
9. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 11.02.2020).
10. *Онопрієнко С.Г.* Класифікація елементів інформаційної культури. Форум права. 2016. № 5. С. 135–138. URL: http://nbuv.gov.ua/UJRN/ FP_index.htm_2016_5_24 (дата звернення 11.02.2020).
11. Цифрова грамотність державних службовців 1.0. на базі інструментів Google. URL: https://osvita.diia.gov.ua/courses/civil-servants (дата звернення 11.04.2020).
12. *Шопіна І.М.* "Запозичена праця": перспективи правового регулювання. Форум права. 2006. № 3. С. 129–135. URL: http://www.nbuv.gov.ua/e-journals/FP/2006-3/06simppr.pdf (дата звернення 11.02.2020).

REFERENCES

1. *Kuzmenko, O.V.* (2009) Pravova determinatsiya ponyattya publichne administruvannya. "Legal Determination of the Concept of Public Administration". Air and Space Law 3, 20–24 [in Ukrainian].
2. *Lukyanets, D.M.* (2012) Formy realizatsiyi derzhavnoyi vlady v suchasniy Ukrayini. "Forms of Realization of State Power in Modern Ukraine". Rule of Law: textbook of scientific works. Issue 23. P. 233–239 [in Ukrainian].
3. *Pylypyshyn, V.P.* (2015) Administratyvnyy aspekt publichnoho administruvannya. "Administrative Aspect of Public Administration". Scientific Notes of the Institute of Legislation of the Verkhovna Rada of Ukraine. No 6. P. 68–71 [in Ukrainian].
4. On the Concept of the National Informatization Program: Law of Ukraine of February 4, 1998 No 75/98-VR. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text (Date of Application: 11.02.2020) [in Ukrainian].
5. *Lytvynenko, O.* (1998) Informatsiya i bezpeka. "Information and Security". New Policy 1, 47–49 [in Ukrainian].
6. *Furashev, V.M.* (2012) Pytannya zakonodavchoho vyznachennya ponyatiyno-katehoriynoho aparatu u sferi informatsiynoyi bezpeky. Issues of Legislative Definition of the Conceptual and Categorical Apparatus in the Field of Information Security. Information and Law 1 (4), 46–56 [in Ukainian].
7. *Kormych, B.A.* (2003) Orhanizatsiyno-pravovi zasady polityky informatsiynoyi bezpeky Ukrayiny. "Organizational and Legal Principles of Information Security Policy of Ukraine": monograph. Odesa: Legal Literature. 472 p. [in Ukrainian].

8. *Zolotar, O.O.* (2011) Klasyfikatsiya informatsiynoyi bezpeky. Informatsiya i pravo. "Classification of Information Security". Information and Law 2, 109–113 [in Ukrainian].
9. On the Basic Principles of Cybersecurity of Ukraine: Law of Ukraine of October 5, 2017 No 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Date of Application: 11.02.2020) [in Ukrainian].
10. *Onopriyenko, S.H.* (2016) Klasyfikatsiya elementiv informatsiynoyi kultury. "Classification of Elements of Information Culture". Law Forum 5, 135–138. URL: http://nbuv.gov.ua/UJRN/FP_index.htm_2016_5_24 (Date of Application: 11.02.2020) [in Ukrainian].
11. Tsyfrova hramotnist derzhavnykh sluzhbovtsiv 1.0. na bazi instrumentiv Google. "Digital Literacy of Civil Servants 1.0. Based on Google Tools". URL: https://osvita.diia.gov.ua/courses/civil-servants (Date of Application: 11.04.2020) [in Ukrainian].
12. *Shopina, I.M.* (2006) "Zapozychena pratsya": perspektyvy pravovoho rehulyuvannya. "Borrowed Labor": Prospects for Legal Regulation". Law Forum 3, 129–135 [in Ukrainian].

UDC 342.951(477)

Onopriienko Stanislav,
Candidate Sci. (Law), Senior Lecturer,
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine,
ORCID ID 0000-0002-5524-1798

INFORMATION SECURITY OF THE PUBLIC ADMINISTRATION

Paper is devoted to the definition of the essence of information security in the sphere of public administration. The definition of public administration is proposed as the activity of state bodies, local self-government bodies and their officials, determined by legislative and subordinate legal acts, aimed at satisfying public interests. Attention is emphasized that the implementation of public administration presupposes the onset of legal responsibility for violation of legal regulations and the application of measures of state, municipal and public control. Relationships in the field of public administration aimed at securing public interest. Public interest in the paper is understood as a set of goals, aspirations, needs that arise from individuals and legal entities in the process of their activities (life), which satisfaction of requires the implementation of legally significant actions by the subjects of public administration.

Research article argues that information security in the field of public administration is a component of national information security, which can be represented as a combination of information security of the legislative and judicial authorities, as well as information security of public administration bodies. At the same time, in accordance with the specifics of the functioning of public administration bodies, threats to information security in their activities can be both external and internal ones. The information security sphere of public administration can also be classified according to the nature of the risks. If the risks are of a technological nature and relate to the security of equipment and programs that use the concept of "cybersecurity". The author has determined that cybersecurity is an integral part of information security, along with personal and corporate information security.

Special attention is drawn to factors that reduce the level of information security in the public administration sphere. These include both external (information and psychological operations aimed at destabilization of the activities of public administration

DOI (Article): https: //doi.org/10.36486/np.2020.2(48).27

bodies, the state of their technological equipment) and internal (the existence of a logical and understandable for any subject of information legal relations of a system of requirements for ensuring information security, as well as the level of information culture of both representatives of public administration bodies and citizens enter into legal relations with them in order to realize their interests) ones.

Keywords: information security, public administration, cyber security, information legal relations, information culture, risks, public administration, information technologies.

Отримано 10.06.2020