ISSN 2072–8670 (Print)
НАУКА І ПРАВООХОРОНА
NAUKA I PRAVOOKHORONA
DOI (Issue): https: //doi.org/10.36486/np.2021.4(54)
Issue 4(54) 2021

УДК 351.746.1(477)

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

ОБ'ЄКТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ

У статті досліджено поняття об'єкта забезпечення інформаційної безпеки у сфері публічного адміністрування. Акцентовано, що зменшення руйнівного впливу інформаційних загроз у системі публічного адміністрування має своєю передумовою підвищення вільної конкуренції на ринку IT-технологій, зміцнення інститутів громадянського суспільства, забезпечення додержання правових приписів у діяльності партій та релігійних організацій, збільшення транспарентності їх діяльності, активізацію цифрової просвіти, подолання цифрової нерівності.

Ключові слова: *інформаційна безпека, публічне адміністрування, об'єкт інформаційної безпеки, суб'єкти інформаційної безпеки, інформаційні загрози, національна безпека.*

Проблема визначення об'єкта соціальної діяльності має беззаперечне значення для побудови ефективного правового механізму останньої. Коректне та науково обґрунтоване визначення виду суспільних відносин або іншого блага, на досягнення (отримання) якого мають бути спрямовані впливи органів публічної влади, громадянського суспільства та інших суб'єктів забезпечення інформаційної безпеки дозволить визначити досяжні цілі та завдання, на які мають бути спрямовані зусилля вказаних суб'єктів, встановити реалістичні критерії оцінки досягнутих результатів. Однак, незважаючи на важливість вирішення вказаного наукового завдання як на теоретичному, так і на практичному рівні, на жаль, воно досі залишається невирішеним. Вказане обумовлює актуальність та новизну теми цієї статті.

Проблеми інформаційної безпеки розглядали у своїх роботах такі вчені, як І. Арістова, О. Баранов, К. Бєляков, В. Богуш, О. Довгань, К. Долженко, О. Золотар, Р. Калюжний, Б. Кормич, Ю. Лісовська, А. Марущак, Н. Новицька, О. Олійник, Т. Перун, Є. Скулиш, О. Тихомиров, Т. Ткачук, В. Цимбалюк, В. Фурашев, О. Шевчук та інші науковці. Проте проблеми інформаційної безпеки в сфері публічного адміністрування ще недостатньо висвітлені на теоретико-методологічному рівні, що обумовлює потребу у подальших наукових пошуках.

Метою статті є визначення поняття та особливостей об'єкта забезпечення інформаційної безпеки у сфері публічного адміністрування.

Гібридний характер сучасних воєн обумовлює підвищення значущості інформаційної безпеки для збереження сталих суспільних відносин, для забезпечення державного суверенітету та територіальної цілісності, створення сприятли-

DOI (Article): https: //doi.org/10.36486/np.2021.4(54).12

вих умов для розвитку громадянського суспільства та держави, реалізації прав і свобод людини та громадянина. Інформаційна безпека як складне соціальне явище постає у багатьох аспектах, серед яких найбільше значення, на нашу думку, мають правовий, технологічний та соціально-психологічний. У правовому аспекті інформаційна безпека являє собою комплекс інформаційно-правових засобів, передусім правових норм, сукупність яких дозволяє поєднувати теорію і практику правового регулювання, досягаючи його цілей. У технологічному аспекті інформаційна безпека становить собою сукупність виробничих операцій, які змінюють наявний стан захищеності інтересів людини, суспільства та органів публічної влади в інформаційній сфері, завдяки перетворенню існуючих або запровадження нових способів та методів інформаційної діяльності. У соціально-психологічному аспекті інформаційна безпека має розумітися як сукупність особистісних характеристик індивідуальних суб'єктів інформаційних відносин, які обумовлюють збільшення або зменшення інформаційних ризиків під час вибору ними варіантів поведінки при здійсненні діяльності в інформаційній сфері.

Об'єкт як загальна філософська категорія та його особливості досить широко висвітлені у теоретичних джерелах, а його сутність в узагальненому вигляді може буде представлена як те (процес, явище, властивість, ознака), на що спрямована активність (активні дії, активна поведінка, вплив, перетворюючі трансформації) суб'єкта. Інакше кажучи, суб'єкт ставить перед собою певну мету і, намагаючись її досягнути, вносить певні зміни у характеристики об'єкта. З тими або іншими варіаціями такий погляд не викликає особливих дискусій, отже, не вважаємо за доцільне зупинятися на цьому питанні детально. Дещо іншою є ситуація із розумінням об'єкта в праві. У правничих науках сформувалося декілька підходів, прихильники кожного з яких активно обстоюють власну позицію щодо сутності цього феномена.

Найбільш поширеним, як нам видається, є розуміння об'єкта як певного виду суспільних відносин. Право як особливий регулятор суспільних відносин справляє на їх виникнення, існування та припинення істотний вплив, отже, позиція, згідно з якою саме суспільні відносини є об'єктом права [1, с. 285], здається нам цілком логічною. Разом з тим об'єкт права не можна, на наше переконання, ототожнювати з об'єктом забезпечення, яким, на нашу думку, є об'єкт забезпечення інформаційної безпеки.

Інші вчені вважають, що об'єктом є певне суспільне благо. Як пише з цього приводу В. Ємельянов, сьогодні у вітчизняній науці кримінального права існує два діаметрально протилежні концептуальні підходи до проблеми об'єкта. Одна концепція об'єктом злочинів визначає сукупність суспільних відносин, інша – блага, цінності та інші сфери життєдіяльності людей. Обидві концепції мають своє історичне коріння та сучасних послідовників. Сам автор вважає визнання об'єктом злочину суспільних відносин з позиції науки недостатньо обґрунтованим, з позиції законодавства – нічим не підтвердженим, а з позиції практики боротьби зі злочинністю – недоцільним [2, с. 175]. Утім сам автор не поділяє і підходу до сутності об'єктів злочинів як певного блага і пропонує розуміти під вказаними об'єктами сфери життєдіяльності людей.

Досить цікавою є позиція Ю. Жорнокуя, який на підставі аналізу думок інших вчених висловлює думку, що під час визначення поняття об'єкта суб'єктивного

цивільного права необхідно дотримуватися визначення об'єкта як того, з приводу чого виникають правовідносини. Зі змістового боку, пише автор, слід вивчати об'єкт будь-якого суб'єктивного права як об'єкт двох видів: безпосередній (найближчий) об'єкт – це належна поведінка суб'єктів правовідношення; опосередкований (матеріальний) об'єкт – це майнові і немайнові блага, з приводу яких і виникають правовідносини [3, с. 108]. Нам імпонує можливість співвіднести таку позицію з практичним аспектом діяльності органів публічного адміністрування, у тому числі й у сфері інформаційної безпеки. Не заперечуючи існування абстрактного суспільного блага, пов'язаного із досягненням високого рівня захищеності інтересів людини, громадянського суспільства, органів публічного адміністрування та інших суб'єктів в інформаційній сфері, зауважимо однак, що світова глобалізація та транскордонність обумовлюють швидкість поширення інформаційних загроз, вплив на виникнення яких від конкретних органів публічного адміністрування може й не залежати (наприклад, у ситуації поширення шкідливого програмного забезпечення, розробленого в умовах максимального фінансового та технологічного сприяння на території держави-агресора). Проте це не означає, що органи публічного адміністрування позбавлені можливості вплинути на ступінь небезпечності вже існуючих загроз шляхом створення безпечних алгоритмів виконання стандартних професійних дій, систематичного навчання персоналу тощо.

Під час визначення об'єкта забезпечення інформаційної безпеки у сфері публічного адміністрування слід пам'ятати, що забезпечення вказаного виду безпеки – це не право як універсальний регулятор і не злочин як особливий делікт, про об'єкти яких йшлося вище. Забезпечення являє собою специфічний вид соціальної діяльності, тобто активності фізичних та юридичних осіб, спрямованої на перетворення оточуючої реальності з метою досягнення поставлених цілей. Головне питання, яке при цьому виникає, – хто саме формулює цілі такої діяльності? З одного боку, безумовно, держава в особі суб'єктів забезпечення національної безпеки, одним із видів якої є інформаційна безпека. Однак якщо б держава виступала основним суб'єктом формулювання цілей інформаційної безпеки, їх виконання та контролю за їх досягненням, Україна швидше давно б втратила інформаційний суверенітет, оскільки 90 % цілей, закладених у численних доктринах, концепціях, стратегіях, програмах, планах у сфері національної безпеки, традиційно не виконуються тими суб'єктами, на яких таке виконання покладено. Проте багатоманітність та плюралізм суб'єктів інформаційної діяльності, динамічний розвиток інформаційних відносин, залучення до сфери інформаційних технологій великої кількості інвестицій обумовлюють автономність вирішення завдання подолання загроз інформаційній безпеці недержавними суб'єктами (суб'єктами господарювання, громадськими організаціями, які отримують гранти для здійснення заходів з медіапросвіти тощо). Долаючи ті загрози інформаційній безпеці, які співвідносяться з їх статутними цілями, такі суб'єкти самостійно формулюють цілі забезпечення інформаційної безпеки, самостійно визначають шляхи та критерії їх досягнення, самостійно фінансують таку діяльність за рахунок своїх прибутків або грантів. У сукупності така діяльність істотно знижує руйнівний вплив інформаційних загроз у державі.

DOI (Article): https: //doi.org/10.36486/np.2021.4(54).12

Це не заперечує цінності діяльності у сфері інформаційної безпеки деяких суб'єктів публічного адміністрування. Однак оцінювання такої діяльності науковими методами у відкритій науковій періодиці навряд чи можливе, оскільки вона охоплюється законодавством про захист державної таємниці або має правовий режим службової інформації з обмеженим доступом. Проте аналіз інформації з відкритих джерел дозволяє стверджувати, що діяльність держави у досліджуваній сфері характеризується непослідовністю та хаотичністю – так, наприклад, на Міністерство інформаційної політики України Доктриною інформаційної безпеки України, затвердженою Указом Президента України від 25 лютого 2017 року № 47/2017, покладається функція моніторингу загроз національним інтересам і національній безпеці в інформаційній сфері. Вказане міністерство було реорганізоване з ліквідацією функцій та повноважень 2 вересня 2019 року, а виконання функції моніторингу інформаційним загрозам на новоутворені Міністерство культури, молоді та спорту України та Міністерство цифрової трансформації України не покладено, і таких прикладів можна наводити ще багато (особливо стосовно багатьох центрів протидії інформаційним загрозам, правовий статус яких не визначено, діяльність практично не фінансується і через деякий час фактично припиняється).

Отже, розуміння цілей забезпечення інформаційної безпеки має свої відмінності залежно від суб'єктів такого забезпечення. Найлегше вивчити особливості цілей державного забезпечення інформаційної безпеки, оскільки вони закріплюються у відповідних доктринах, стратегіях, програмах і планах, однак їх виконання органами публічної влади має переважно формальний характер. Складніше простежити особливості формулювання цілей забезпечення інформаційної безпеки суб'єктами господарської діяльності, оскільки вони можуть бути віднесені до комерційної таємниці, та громадськими організаціями, оскільки вони оприлюднюють результати своєї діяльності перед широким загалом у добровільному порядку. Однак у будь-якому разі можна стверджувати, що цілі забезпечення інформаційної безпеки мають багаторівневий характер, формулюються різними суб'єктами, можуть суперечити одне одному, при цьому єдиний центр управління, який би відстежував формулювання і досягнення таких цілей, відсутній.

За таких умов казати про єдиний і загальновизнаний перелік благ, які складали б об'єкт інформаційної безпеки, було б, на нашу думку, некоректним (так, для суб'єктів господарювання благом може вважатися відсутність жодного впливу держави на їх виробничі та організаційно-управлінські процеси, натомість, для органів публічного управління благом може вважатися контроль над поширенням певних видів інформації). Така ситуація притаманна не лише Україні, а й іншим державам [4].

Заслуговує на увагу думка О. Тихомирова, який вважає, що інтегруючою основою змісту діяльності із забезпечення інформаційної безпеки є такі її елементи, як об'єкт, предмет, суб'єкт, мета, засоби, методи, принципи, результати. При цьому об'єкти національної та інформаційної безпеки, на його думку, є спільними – особа, суспільство, держава; загальними об'єктами державного забезпечення інформаційної безпеки є інформаційна інфраструктура (держави, суспільства) та свідомість (особи, суспільства) [5, с. 191]. Ми підтримуємо думку

вченого про можливість виокремлення об'єктів державного забезпечення інформаційної безпеки. Разом з ними, як нам здається, можна виділити ще об'єкти громадського, муніципального та господарсько-правового забезпечення інформаційної безпеки, кожен з яких буде мати свої особливості.

На підставі здійсненого аналізу можна зробити такі висновки. Об'єкт забезпечення інформаційної безпеки являє собою мету, яку ставить перед собою суб'єкт діяльності у вказаній сфері (держава та її органи, органи місцевого самоврядування, суб'єкти господарювання, громадські організації, політичні партії, професійні спілки, релігійні організації, окремі громадяни тощо). Найменш ефективним із заначених суб'єктів є держава, що пояснюється як традиційною для української реальності непослідовністю державної інформаційної політики, так і надмірною динамічністю технічних, технологічних, кадрових, організаційних та інших процесів в інформаційній сфері, що утруднює їх централізоване регулювання. Отже, об'єкт забезпечення інформаційної безпеки постає як множинність неузгоджених між собою об'єктів різної генези та масштабу, сукупність яких породжує міцність протидії інформаційним ризикам, компенсуючи тим самим слабкість держави у досліджуваній сфері суспільних відносин. Звідси випливає, що зменшення руйнівного впливу інформаційних загроз у системі публічного адміністрування має своєю передумовою підвищення вільної конкуренції на ринку IT-технологій, зміцнення інститутів громадянського суспільства, забезпечення додержання правових приписів у діяльності партій та релігійних організацій, збільшення транспарентності їх діяльності, активізацію цифрової просвіти для всіх категорій здобувачів освіти, подолання цифрової нерівності. У поєднанні з функціонуванням вузькоспеціалізованих підрозділів із забезпечення інформаційної та кібербезпеки у структурі деяких суб'єктів публічного адміністрування сектору безпеки і оборони це, на нашу думку, здатне значно оптимізувати ситуацію із подолання руйнівного впливу інформаційних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Алексеев С.С.* Об объекте права и правоотношения. Вопросы общей теории советского права. Москва: Юрид. лит, 1960. С. 284–306.

2. *Ємельянов В.П.* Дискусійні питання щодо визначення об'єкта злочину у кримінально-правовій науці. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2007. № 16. С. 172–182.

3. *Жорнокуй Ю.М.* Об'єкт корпоративного правовідношення. *Юридична наука*. 2011. № 2. С. 106–111.

4. *Khomiakov D., Khrystynchenko N., Shopina I., Zhukov S., Shpenov D.* Cybersecurity: Legal and Organizational Support in Leading Countries, NATO and EU Standards. *Journal of Security & Sustainability Issues*. 2020/3/1. Volume 9, Issue 3. P. 977–992.

5. *Тихомиров О.О.* Забезпечення інформаційної безпеки як функція держави: дис. ... канд. юрид. наук: 12.00.01. Київ, 2011. 234 с.

REFERENCES

1. *Alieksieiev S.S.* (1960). Ob obekte prava i pravootnosheniia. "On the object of law and legal relations". Questions of the general theory of Soviet law. Moscow: Yurid.lit. P. 284–306. [In Russian].

2. *Yemielianov V.P.* (2007). Dyskusiini pytannia shchodo vyznachennia obiektu zlochynu u kryminalno-pravovii nautsi. "Debatable issues regarding the definition of the object of crime in

criminal law science". Fight against organized crime and corruption (theory and practice). No. 16. P. 172–182. [In Ukrainian].

3. *Zhornokui Yu.M.* (2011). Obiekt korporatyvnoho pravovidnoshennia. "Object of corporate legal relationship". Juridical science. No. 2. P. 106–111. [In Ukrainian].

4. *Khomiakov D., Khrystynchenko N., Shopina I., Zhukov S., Shpenov D.* Cybersecurity: Legal and Organizational Support in Leading Countries, NATO and EU Standards. Journal of Security & Sustainability Issues. 2020/3/1. Volume 9, Issue 3. P. 977–992. [In English].

5. *Tykhomyrov O.O.* (2011). Zabezpechennia informatsiinoi bezpeky yak funktsiia derzhavy. "Ensuring information security as a function of the state": dis. Cand. Jurid. Sciences: 12.00.01. Kyiv. 234 p. [In Ukrainian].

UDC 351.746.1(477)

Onopriienko Stanislav,
Candidate of Juridical Sciences, Senior Lecturer,
Taras Shevchenko National University of Kyiv,
Kyiv, Ukraine,
ORCID ID 0000-0002-5524-1798

OBJECT OF ENSURING INFORMATION SECURITY IN THE SPHERE OF PUBLIC ADMINISTRATION

The purpose of the article is to define the concept and features of the object of information security in the field of public administration.

The article deals with the peculiarities of understanding the category of "object" in the legal science. Considered scientific approaches, according to which under the object of law means social relations, goods and values. Accentuated that security is a specific type of social activity, that is, the activity of individuals and legal entities aimed at transforming the surrounding reality to achieve their goals.

Author propose to understand the object of ensuring information security as a goal set by the subject of activity in this area (the state and its bodies, local authorities, business entities, public organizations, political parties, trade unions, religious organizations, individual citizens, etc.).The least effective of these subjects is the state, which is explained both by the inconsistency of the state information policy, which is traditional for Ukrainian reality, and by the excessive dynamism of technical, technological, personnel, organizational and other processes in the information sphere, which complicates their centralized regulation. It is argued that the object of ensuring information security acts as a plurality of inconsistent objects of different genesis and scale, the combination of which gives rise to the strength of countering information risks, thereby compensating for the weakness of the state in the studied sphere of public relations. Therefore, it follows that the reduction of the destructive impact of information threats in the system of public administration is due to the strengthening of free competition in the market of IT technologies, strengthening of civil society institutions, enforcement of legal norms in the activities of parties and religious organizations. The government must take into account the fact that the digital education of all categories of applicants for education and bridging the digital divide are becoming more and more transparent. In combination with the functioning of

highly specialized divisions for information and cyber security in the structure of some subjects of public administration of the security and defense sector, this, in our opinion, can significantly optimize the situation with overcoming the destructive influence of information threats.

Keywords: information security, public administration, information security object, subjects of information security, information threat, national security.

Отримано 30.11.2021