ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СФЕРИ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ

Станіслав Григорович ОНОПРІЄНКО,

кандидат юридичних наук,
викладач кафедри правового забезпечення
Військового інституту Київського національного
університету імені Тараса Шевченка

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 [1, с. 112]. Спробуємо знайти місце інформаційної безпеки суб'єктів публічного адміністрування відповідно до наведеної класифікації.

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, уявляє 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 носять 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 [2]. 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 [3, 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») [4], а й передбачало б напрацювання державними службовцями та службовцями органів місцевого самоврядування практичних навичок у сфері інформаційної безпеки. Для забезпечення викривлення результатів такого навчання з-за впливу корпоративної солідарності і сам процес навчання, і оцінювання його результатів мало б здійснюватися незалежними суб'єктами на принципах аутсорсингу або «запозиченої праці» [5].

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. Золотар О. О. Класифікація інформаційної безпеки. *Інформація і право.* 2011. № 2. С. 109-113.

2. 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).

3. 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).

4. Цифрова грамотність державних службовців 1.0. на базі інструментів Google. URL: https://osvita.diia.gov.ua/courses/civil-servants (дата звернення 11.04.2020)

5. 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).