УДК 65.012.8:007+32(477)
DOI https://doi.org/10.32782/ln.2023.21.11

Недохлєбов І.І.
здобувач кафедри конституційного та адміністративного права
Запорізький національний університет

АНАЛІЗ ОРГАНІЗАЦІЙНО-ПРАВОВИХ ФОРМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Розвиток теорії інформаційного права є необхідною умовою формування вчення про інформаційну безпеку. З огляду на це, осмислення природи та змісту деяких категорій також має принципове значення. Однією з таких категорій є форми, які прийнято вважати складовою адміністративно-правового механізму забезпечення інформаційної безпеки. На сучасному етапі ця категорія недостатньо дослідження науковцями, що не дозволяє у повній мірі використовувати її потенціал в рамках розбудови системи інформаційної безпеки. Тому тема цієї статті може вважатися актуальним напрямком наукового пошуку.

Аналіз останніх досліджень і публікацій з даної теми, виділення невирішених раніше частин загальної проблеми, яким присвячується дана стаття. Окремі форми забезпечення інформаційної безпеки України в різні часи досліджували: Є. В. Валькова, В. К. Галіцин, О. С. Дніпров, О. В. Кологойда, Є. А. Макаренко, В. І. Пожуєв, О. М. Поляков, О. М. Селезньова, О. П. Суслов, Н. К. Самченко, О. С. Яра та інші вчені. Однак, з урахуванням динамічного розвитку системи інформаційної безпеки та появи нових загроз, їхні наукові праці частково втратили актуальність.

Метою статті є комплексний аналіз організаційно-правових форм забезпечення інформаційної безпеки України.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Є. В. Валькова зазначає, що за правовими наслідками форми забезпечення інформаційної безпеки слід класифікувати на правові та організаційні. Правові форми тягнуть за собою юридичні наслідки й здатні змінювати правове становище суб'єктів, які є учасниками відносин у сфері інформаційної безпеки, або змінювати саму інформаційну сферу. Своєю чергою організаційні форми такого навантаження не несуть, мають забезпечувальний характер щодо протікання управлінських процесів у сфері забезпечення інформаційної безпеки [1, с. 62]. Вбачається, що форми представляють собою поєднання правових та організаційних засобів, які використовуються в діяльності розпорядчих та контролюючих суб'єктів інформаційної безпеки з метою забезпечення додержання законодавства в цій сфері, а також гарантування належного рівня захищеності національних інтересів держави, суспільства та особистості.

На нашу думку, форми є деталізацією методів забезпечення інформаційної безпеки, адже вони конкретизують характер та напрями організаційно-розпорядчого впливу. Аналіз законодавства у сфері інформаційної безпеки дозволяє до числа правових форм віднести видання нормативно-правових актів та актів індивідуальної дії, а також здійснення контролю та моніторингу окремих сфер інформаційної діяльності. До числа організаційних форм слід зарахувати формування і реалізацію інформаційної політики держави та міжнародне співробітництво у сфері захисту інформації. Схарак-

теризуємо кожну форму забезпечення інформаційної безпеки окремо.

1. Видання нормативно-правових актів та актів індивідуальної дії. Ця форма передбачена для вирішення двох важливих завдань: регламентація інформаційних правовідносин (у тому числі безпекової складової); реагування на неправомірні дії окремих учасників цих правовідносин. О. С. Дніпров зауважує, що видання нормативних актів як форма діяльності центральних органів виконавчої влади – це зовнішньо виражена форма правотворчої діяльності органів влади, яка здійснюється шляхом встановлення правових норм на нормативно-правовому рівні відповідно до положень Конституції України та законів України та спрямована на врегулювання суспільних відносин у певній галузі/сфері життєдіяльності [2, с. 145]. Тобто, шляхом нормотворчості відбувається формалізація механізмів захисту інтересів держави, суспільства та особистості на основі індивідуалізації сфер інформаційної діяльності.

З цього приводу О. С. Яра стверджує, що видання нормативно-правових актів, як інструмент забезпечення інформаційної безпеки в Україні – це розпорядча правотворча адміністративна діяльність загальних суб'єктів публічної адміністрації з метою уточнення деталізації законів України до моменту їх правозастосування шляхом утвердження вторинних норма права, загальнообов'язкових для не персоніфікованих осіб, які приймають участь в адміністративно правових відносинах в інформаційній сфері [3, с. 51]. Слід частково погодитися з таким твердженням, адже мова йде про нормотворчість не тільки на підзаконному рівні, але й на законодавчому. Тому досліджувана форма значно ширше за своїм змістом, що дозволяє більш комплексно підходити до формування системи інформаційної безпеки.

За своїм характером акти індивідуальної дії суттєво відрізняються від нормотворчості. Відповідно до Інформаційного листа Вищого адміністративного суду України від 01 червня 2010 року № 781/11/13-10 «Щодо застосування окремих норм матеріального права під час розгляду адміністративних спорів», акти індивідуальної дії представляють собою правозастосовний акт, який містить конкретизовані суб'єктами адміністративного права вимоги, звернені до особи або групи осіб. Особливість таких актів полягає в тому, що вони можуть бути оскаржені лише особами, безпосередні права, свободи чи охоронювані законом інтереси яких такими актами порушені. При цьому, нормативно-правові акти можуть бути оскаржені широким колом осіб (фізичних та юридичних), яких вони стосуються [4].

Отже, основна відмінність в тому, що нормативно-правові акти формуються на основі індивідуалізації сфер діяльності, а індивідуальні акти – на основі персоналізації суб'єкта. У якості прикладу розглянемо Постанову Подільського районного суду м. Києва від 07 лютого 2020 року по Справі № 758/14158/19. В матеріалах справи фігурує саме такий акт індивідуальної дії – протокол про адміністративне правопорушення від 04 листопада 2019 року, складений представника Уповноваженого Верховної Ради України з прав людини. Мова йде про притягнення до адміністративної відповідальності посадової особи Вищої школи адвокатури Національної асоціації адвокатів України за статтею 189-39 Кодексу України про адміністративні правопорушення (порушення статті 29 Закону України від 01 червня 2010 року № 2297-VI «Про захист персональних даних») [5]. Означений акт індивідуальної дії є реакцією на загрози інформаційній безпеці особистості, оскільки втрата персональної інформації може мати дуже негативні наслідки для суб'єкта персональних даних.

2. Контроль та моніторинг окремих сфер інформаційної діяльності. Ця форма використовується з подвійною метою: по-перше, для прогнозування потенційних загроз інформаційній безпеці; по-друге, для попередження правопорушень суб'єктами інформаційних

правовідносин. О. В. Кологойда зазначає, що контроль представляє собою діяльність уповноважених законом центральних органів виконавчої влади, їх територіальних органів, органів місцевого самоврядування, інших органів у межах повноважень, передбачених законом, щодо виявлення та запобігання порушенням вимог інформаційного законодавства та забезпечення інтересів держави, суспільства та особистості в інформаційній сфері [6, с. 50]. На нашу думку, рівень забезпечення інформаційної безпеки напряму залежить від цієї форми, адже вона дозволяє забезпечити потужний превентивний ефект.

В інформаційній сфері досліджувана форма реалізується на основі індивідуалізації окремих сфер інформаційної діяльності. Так, у Законі України від 13 грудня 2022 року № 2849-IX «Про медіа» встановлено, що контроль у сфері медіа використовується з метою забезпечення дотримання на території України вимог і обмежень у сфері медіа, захисту національного медіа-простору України та побудови інформаційного середовища, здатного протистояти актуальним загрозам інформаційній безпеці [7]. В свою чергу, Постанова Правління Національного банку України від 16 січня 2021 року № 4 «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг» регламентує порядок організації та здійснення заходів контролю за дотриманням банками вимог законодавства, яке регулює відносини у сферах кіберзахисту, інформаційної безпеки та електронних довірчих послуг, а також вимоги щодо проведення банком самооцінки стану інформаційної безпеки [8]. Вочевидь, індивідуалізація забезпечує формування особливого підходу до виявлення та попередження протиправної діяльності, яка становить загрозу інформаційній безпеці.

В теорії адміністративного права моніторинг позиціонується як процес системного відстеження та збирання даних про об'єкт управлінської діяльності, зокрема чинники, що впливають на нього, з метою ефективного впливу суб'єкта управління на означений об'єкт. При чому моніторинг має розв'язати проблему забезпечення контролю достовірною інформацією, тобто він виконує інформаційно-аналітичну функцію [9, с. 72]. Вбачається, що моніторинг в системі інформаційної безпеки виступає допоміжною формою, яка забезпечує владно-розпорядчий вплив.

Слід зауважити, що ця форма реалізується не тільки суб'єктами владних повноважень, оскільки передбачено можливість проведення моніторингу інститутами громадянського суспільства. Як правило, подібний моніторинг стосується окремих безпекових питань та полягає у незалежній оцінки ситуації та формуванні рекомендацій органам виконавчої влади. До прикладу наведемо Звіт про моніторинг стану забезпечення інформаційних прав в умовах воєнного стану від 2022 року. В документі наголошено на декількох принципових речах: 1) наявність проблем, які пов'язані з наданням органами влади публічної інформації громадянам; 2) зростання потреб громадян у комунікаціях із суб'єктами владних повноважень в умовах воєнного стану; 3) необхідність підвищення рівня обізнаності відповідальних працівників органів виконавчої влади [10, с. 54].

3. Формування і реалізація інформаційної політики держави. Ця форма має важливе значення для забезпечення інформаційної безпеки, адже мова йде про розробку та впровадження комплексних напрямків, які містять і безпекову складову та у сукупності утворюють національну інформаційну систему. В. І. Пожуєв зазначає, що основними задачами державної інформаційної політики в сучасних умовах є: 1) модернізація інформаційної інфраструктури; 2) розвиток інформаційних, телекомунікаційних технологій; 3) ефективне формування і використання інформаційних ресурсів та забезпечення широкого, вільного доступу до них; 4) забезпечення громадян суспільно значущою інформацією та розви-

ток незалежних медіа; 5) підготовка людини до життя і роботи в інформаційному столітті; 6) створення необхідної нормативної правової основи побудови інформаційного суспільства [11, с. 8]. Вказані задачі безпосередньо пов'язані з безпековим рівнем, оскільки дозволяють мінімізувати ризики виникнення окремих загроз, а у разі їх виникнення, створюють умови для локалізації наслідків.

У своїй науковій праці О. М. Селезньова припускає, що інформаційна політика повинна закласти основи для вирішення фундаментальних завдань розвитку суспільства, головними з яких є формування єдиного інформаційного простору України та її входження у світовий інформаційний простір, гарантування інформаційної безпеки особистості, суспільства й держави [12, с. 271]. Задля цього, у вітчизняному законодавстві сформовані відповідні напрями інформаційної політики, основним з яких є: забезпечення доступу громадянам до інформації; створення національних систем і мереж інформації; забезпечення ефективного використання інформації; сприяння постійному оновленню та зберіганню національних інформаційних ресурсів; створення загальної системи охорони інформації.

4. Міжнародне співробітництво у сфері захисту інформації. Необхідність цієї форми доволі вдало пояснює О. М. Фролова. Вона наголошує, що транскордонний характер інформаційних загроз змушує країни світу тісно взаємодіяти між собою. Особливою ефективністю вирізняється співпраця в рамках міжнародних організацій, які мають більший потенціал для боротьби з означеними загрозами, систему швидкого реагування на них, на основі яких можна обмінюватися досвідом та приймати рішення глобального характеру. Дослідниця зауважує, що тільки в рамках такої співпраці можна напрацювати універсальні правила, принципи та норми відповідальності за інформаційні правопорушення [13, с. 134]. Тобто, співробітництво виступає у якості інструмента удосконалення вітчизняної системи забезпечення інформаційної безпеки, розширення її функціонального потенціалу за рахунок використання позитивного зарубіжного досвіду.

В свою чергу Є. А. Макаренко також наголошує, що ефективність боротьби з загрозами в інформаційній сфері залежить не тільки від заходів, які здійснюються на рівні національних інституцій, правоохоронних органів, інших установ і організацій, на які покладено загальні завдання забезпечення інформаційної безпеки, але й від координації політики і співпраці держав на багатосторонній основі в кожному регіону світу. Науковець окреслює наступні перспективні механізми такої співпраці: взаємні консультації, координація співпраці, кооперація в наукових дослідженнях, розробка і виробництво відповідних засобів захисту інформації, а також виконання державами заходів згідно з прийнятими на себе міжнародними зобов'язаннями [14, с. 61].

О. М. Поляков конкретизує сучасні напрямки міжнародного співробітництва з ООН у сфері забезпечення інформаційної безпеки, до числа яких науковець відносить: 1) уніфікація правил, норм та принципів поведінки держав в інформаційному просторі; 2) впровадження заходів спрямованих на зміцнення довіри до цього простору; 3) пошук шляхів нарощування цифрового потенціалу; 4) інституціоналізація переговорного механізму з питань міжнародної інформаційної безпеки. З огляду на це автор вважає перспективною участь України у роботі міжнародної платформи Програми дій із заохочення відповідальної поведінки держав у кіберпросторі Генеральної Асамблеї ООН та Групи урядових експертів ООН з питань інформаційної безпеки (UNGGE) [15, с. 133].

Однак, це лише окремий напрямок міжнародного співробітництва в інформаційній сфері, окрім якого існує ще співпраця на міжвідомчому та міжгалузевому рівнях. Прикладом такої співпраці є Меморандум між Міністерством цифрової трансформації України та Європейською організацією

кібербезпеки (ECSO), який був підписаний у 2022 році. Документ дозволяє: посилити систему кіберзахисту України; забезпечити доступ українських підприємств та фахівців до ринку кібербезпеки ЄС та навчальних ресурсів; організувати просування українських стартапів у сфері кіберзахисту; забезпечити підтримку науково-технічних проєктів [16].

Висновки з дослідження і перспективи подальших розвідок у даному науковому напрямку. Таким чином, в рамках механізму адміністративно-правового забезпечення інформаційної безпеки застосовується поєднання правових та організаційних форм, які дозволяють врегулювати безпекові питання через владно-розпорядчий вплив на дві категорії об'єктів управління. До першої категорії слід віднести питання, які перебувають у центрі системи інформаційної безпеки (умови реалізації права на інформацію, механізми захисту означеного права, деталізація процедурних питань задоволення інформаційних потреб, встановлення правових режимів доступу до інформації тощо). До другої категорії належать відносини, які перебувають на периферії системи інформаційної безпеки, але важливі для досягнення її належного рівня (розбудова міжнародної співпраці в інформаційній сфері, формування інформаційної політики, розвиток інформаційно-телекомунікаційних систем тощо). Означені форми є невід'ємним елементом методології забезпечення інформаційної безпеки, адже дозволяють конкретизувати виконавчо-розпорядчі методи діяльності суб'єктів інформаційної безпеки, надавши їм чіткого правового змісту та організаційної спрямованості. Перспективним напрямком подальшого наукового пошуку залишається опрацювання методів, які також є складовим елементом адміністративно-правового механізму забезпечення інформаційної безпеки України.

Анотація

У статті здійснено комплексний аналіз організаційних та правових форм забезпечення інформаційної безпеки України. Автор наголошує на проблемі неналежного наукового опрацювання цих категорій, що гальмує розвиток теорії інформаційного права та вчення про інформаційну безпеку як складову національної безпеки України. Зазначено, що форми забезпечення інформаційної безпеки представляють собою поєднання правових та організаційних засобів, які використовуються в діяльності розпорядчих та контролюючих суб'єктів з метою забезпечення законності та гарантування належного рівня захищеності національних інтересів держави, суспільства та особистості в інформаційній сфері. Автор доходить висновку, що означені форми є деталізацією методів забезпечення інформаційної безпеки, адже вони конкретизують характер та напрями організаційно-розпорядчого впливу. Систематизовано та досліджено наступні організаційно-правові форми: видання нормативно-правових актів та актів індивідуальної дії; здійснення контролю та моніторингу окремих сфер інформаційної діяльності; формування і реалізацію інформаційної політики держави; міжнародне співробітництво у сфері захисту інформації. Доведено, що адміністративно-правові форми дозволяють врегулювати безпекові питання через владно-розпорядчий вплив на дві категорії об'єктів управління: відносини, які перебувають у центрі системи інформаційної безпеки та відносини, які перебувають на периферії системи інформаційної безпеки. Обґрунтовано, що досліджені автором форми є невід'ємним елементом методології забезпечення інформаційної безпеки, адже дозволяють конкретизувати виконавчо-розпорядчі методи діяльності суб'єктів інформаційної безпеки, надавши їм чіткого правового змісту та організаційної спрямованості.

Ключові слова: адміністративно-правовий механізм, виклики, загрози, інформаційна безпека, інформаційне законодавство, організаційні форми, правові форми.

Nedokhlebov I.I. Analysis of organizational and legal forms of ensuring information security of Ukraine

Summary

In the article, a comprehensive analysis of organizational and legal forms of ensuring information security of Ukraine is carried out. The author emphasizes the problem of improper scientific study of these categories, which inhibits the development of the theory of information law and the doctrine of information security as a component of Ukraine's national security. It is noted that the forms of ensuring information security represent a combination of legal and organizational means used in the activities of administrative and controlling entities in order to ensure legality and guarantee the appropriate level of protection of the national interests of the state, society and the individual in the information sphere. The author comes to the conclusion that the specified forms are details of the methods of ensuring information security, because they specify the nature and directions of organizational and administrative influence. The following organizational and legal forms were systematized and researched: issuance of regulatory and legal acts and acts of individual action; implementation of control and monitoring of certain spheres of information activity; formation and implementation of the information policy of the state; international cooperation in the field of information protection. It has been proven that administrative and legal forms allow for the settlement of security issues through the power and administrative influence on two categories of management objects: relations that are at the center of the information security system and relations that are at the periphery of the information security system. It is justified that the forms researched by the author are an integral element of the methodology of ensuring information security, because they allow specifying the executive and administrative methods of activity of information security subjects, giving them a clear legal meaning and organizational orientation.

Key words: administrative and legal mechanism, challenges, threats, information security, information legislation, organizational forms, legal forms.

Список використаних джерел:

1. Валькова Є. В. Форми адміністративно-правового регулювання у сфері охорони права інтелектуальної власності. *Право і безпека*. 2012. № 5 (47). С. 61–64.
2. Дніпров О. С. Видання нормативних актів як форма діяльності центральних органів виконавчої влади в Україні. *Підприємництво, господарство і право*. 2020. № 12. С. 143–147.
3. Яра О. С. Видання нормативно-правових актів, як інструмент публічного адміністрування забезпечення вищої юридичної освіти в Україні. *Юридична наука*. 2020. № 10. С. 47–53.
4. Щодо застосування окремих норм матеріального права під час розгляду адміністративних спорів: Інформаційний лист Вищого адміністративного суду України від 01 червня 2010 р. № 781/11/13-10. URL: https://zakon.rada.gov.ua/laws/show/v781_760-10#Text (дата звернення: 16.12.2023).
5. Постанову Подільського районного суду м. Києва від 07 лютого 2020 року по Справі № 758/14158/19. URL: https://zakononline.com.ua/court-decisions/show/87632133 (дата звернення: 19.12.2023).
6. Кологойда О. В. Контроль як правова форма державного регулювання господарських відносин на фондовому ринку України. *Право та інновації*. 2015. № 3 (11). С. 50–58.
7. Про медіа: Закон України від 13 грудня 2022 р. № 2849-IX. *Урядовий кур'єр*. 2023. № 18.
8. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих

послуг: Постанова Правління Національного банку України від 16 січня 2021 р. № 4. *Офіційний вісник України*. 2021. № 11. стор. 82. стаття 470.
9. Галіцин В. К., Суслов О. П., Самченко Н. К. Система моніторингу: навч. посібник. Київ: КНЕУ. 2015. 409 с.
10. Олексіюк Т. О., Кабанов О. М. Звіт про моніторинг стану забезпечення інформаційних прав в умовах воєнного стану 2022 року. Київ. 2022. 62 с.
11. Пожуєв В. І. Формування концепції державної інформаційної політики в умовах глобалізації. *Гуманітарний вісник ЗДІА*. 2010. № 43. С. 4–12.
12. Селезньова О. М. Теоретико-методологічні основи інформаційного права України: монографія. Чернівці: Місто. 2014. 408 с.
13. Фролова О. М. Міжнародне співробітництво у галузі забезпечення інформаційної безпеки. *Вісник Львівського університету*. 2019. № 146. С. 131–136.
14. Макаренко Є. А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. *Актуальні проблеми міжнародних відносин*. 2011. № 102. С. 51–62.
15. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2 (37). С. 129–138.
16. Міністерство цифрової трансформації України та Європейська організація кібербезпеки (ECSO) уклали меморандум про співробітництво. URL: https://khoda.gov.ua/posilju%D1%94mo-k%D1%96berbezpeku-ukra%D1% 97ni%3A-m%D1%96ncifra-ta-ecso-p%D1%96dpisali-memorandum-pro-sp%D1 %96vpracju (дата звернення: 20.12.2023).