УДК 65.012.8:007+32(477)
DOI https://doi.org/10.32782/yuv.v6.2023.32

І. Недохлєбов,
здобувач кафедри конституційного та адміністративного права
Запорізького національного університету

ПРОБЛЕМИ ВИЗНАЧЕННЯ ПЕРСПЕКТИВНИХ НАПРЯМІВ РОЗВИТКУ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Постановка проблеми. Сучасний контекст розвитку інформаційної системи України характеризується наявністю численних загроз, нейтралізація яких вимагає постійного удосконалення організаційно-правових засад забезпечення інформаційної безпеки. Необхідність розробки відповідних шляхів також зумовлена динамічністю останньої, яка обумовлена не тільки загрозами, а й науково-технічним прогресом. Потреба удосконалення системи інформаційної безпеки також обумовлена зростанням ролі громадянського суспільства в сфері інформаційної діяльності. Означені чинники зумовили вибір теми цієї статті.

Аналіз останніх досліджень і публікацій. Окремі питання розвитку системи забезпечення інформаційної безпеки України в різні часи досліджували: Р. О. Басенко, І. І. Килимник, О. І. Крюков, А. П. Кравченко, С. О. Лисенко, О. М. Солодка, В. Л. Смєсова, О. А. Троянський, Р. І. Шаравара, Н. Є. Федорова та інші вчені. Однак, з урахуванням нових загроз та викликів, а також тенденцій реформування сектора безпеки і оборони, їхні наукові праці частково втратили актуальність.

Метою статті є комплексний аналіз перспективних напрямів розвитку системи інформаційної безпеки України.

Виклад основного матеріалу. Процес удосконалення організаційно-правових аспектів забезпечення інформаційної безпеки має відбуватися з урахуванням наступних цілей: максимальне залучення громадянського суспільства до процесів захисту інформації на усіх рівнях інформаційної безпеки; встановлення балансу між приватністю та національними інтересами в інформаційній сфері; врахування контексту збройного конфлікту як вагомого чинника, що впливає на розвиток сучасної системи інформаційної безпеки; врахування неможливості кодифікації інформаційного законодавства та різноплановості окремих сфер інформаційної діяльності; недопущення випадків дублювання повноважень владно-розпорядчих суб'єктів в сфері інформаційної безпеки; недопущення конфлікту інтересів між урядовими та неурядовими суб'єктами інформаційної безпеки; чітке позиціонування інтересів держави, суспільства та особистості в сфері інформаційної безпеки.

У наукових колах питання удосконалення системи інформаційної безпеки дискутується доволі активно. При чому, в науці інформаційного права сформувалося декілька підходів до бачення напрямів удосконалення організаційно-правових засад розвитку зазначеної системи. Для їхньої візуалізації слід проаналізу-

вати наукові праці деяких вчених. Наприклад, О. А. Троянський систематизує наступні перспективні шляхи удосконалення системи інформаційної безпеки: 1) законодавче врегулювання окремих питань захисту інформації; 2) забезпечення законності та дисципліни посадовими особами органів влади; 3) виключення випадків бездіяльності уповноважених органів; 4) належне реагування на виклики сьогодення у правовий спосіб; 5) покращення координації дій між органами державної влади, місцевого самоврядування, недержавними структурами і громадянами з питань забезпечення інформаційної безпеки [1, с. 190].

Слід констатувати, що дослідник здебільшого акцентує увагу на організаційно-правових аспектах розвитку системи інформаційної безпеки, надаючи їм пріоритет. Схожої позиції дотримується І. І. Килимник, який до числа перспективних форм розвитку системи інформаційної безпеки пропонує відносити: забезпечення ґрунтовності та системності відповідної політики держави; забезпечення злагодженого функціонування суб'єкта інформаційної безпеки; створення спеціально уповноваженого органу з питань інформаційної безпеки; залучення до усіх процесів недержавних суб'єктів [2, с. 57]. На нашу думку, домінування організаційно-правових аспектів обумовлене прагненням впорядкувати політику держави у сфері національної безпеки, і зокрема її інформаційної складової.

О. І. Крюков наголошує, що актуальним практичним завданням залишається досягнення єдиного підходу до визначення оптимальних моделей і шляхів забезпечення інформаційної безпеки держави на основі виявлення найважливіших якісних і кількісних властивостей та параметрів цього явища [3, с. 109]. Ця теза вказує на важливість оцінки ефективності системи інформаційної безпеки, яка є умовою захисту інтересів держави, суспільства та особистості в інформаційній сфері. Також науковець підтверджує думку автора цього дослідження про те, що окремого виду державної політики, у нашому випадку не достатньо. Ми повинні орієнтуватися на унікальну організаційно-правову модель забезпечення інформаційної безпеки, яка матиме власні ідеологічні засади. У цьому сенсі, слід погодитися з С. О. Лисенко, який наголошує на необхідності побудови такої системи інформаційної безпеки, яка буде заснована на принципах гармонійного співвідношення та взаємодії державного впливу та недержавних організацій [4, с. 171]. Втім є інший підхід, який переважно сконцентрований на удосконалення нормативно-правової складової.

Так, Р. О. Басенко, Р. І. Шаравара та А. П. Кравченко обґрунтовують наступні перспективні форми удосконалення системи інформаційної безпеки: 1) збереження незалежного та вільного інформаційного простору; 2) здійснення контролю над поширенням дезінформації; 3) удосконалення інформаційного законодавства; 4) формування цілісної стратегії протидії інформаційній війні; 5) підвищення медійної грамотності громадян; 6) обмеження впливу інформаційних ресурсів, що діють на користь ворога; 7) збільшення рівня свідомості населення шляхом інформування його про ситуацію в країні із достовірних джерел інформації [5, с. 30].

Цей підхід частково простежується в окремих підзаконних актах. Зокрема, у Концепції технічного захисту інформації в Україні, затвердженої Постановою Кабінету Міністрів України від 08 жовтня 1997 року № 1126, закріплено наступні перспективні форми діяльності: розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави; удосконалення правових механізмів організаційного забезпечення; розроблення нормативних

документів з питань формування та розвитку моделі загроз для інформації [6]. Варто зазначити, що вказана вище концепція втратила свою актуальність через появу нових загроз та зміни національного контексту. Тому, підхід орієнтований виключно на законодавчі зміни, не відповідає реальному стану розвитку системи інформаційної безпеки.

Наступний підхід щодо розуміння перспектив розвитку організаційно-правових засад інформаційної безпеки заснований на протидії негативного інформаційного впливу на суспільство та особистість. Він передбачає, що реформування та розвиток інформаційно-освітнього простору потребує цілеспрямованого формування сучасного інформаційно-освітнього середовища, педагогічно виваженого проектування та використання комп'ютерно-орієнтованих методичних систем навчання, а також відповідного удосконалення системи підготовки та підвищення кваліфікації працівників навчальних закладів, наукових установ та органів управління освітою.

В рамках цього підходу Н. Є. Федорова та В. Л. Смєсова акцентують увагу на проблемі випереджувального розвитку форм, способів, технологій і методик впливу на свідомість або підсвідомість, психічний стан людини порівняно з темпами формування й удосконалення методів та інструментів протидії відповідним деструктивним психологічним впливам. З огляду на це, науковці пропонують сконцентруватися на протидії дезінформації, залякування, емоційного придушення, ініціювання агресивних емоційних станів та маніпуляції [7, с. 15]. Отже, мова йде про розбудову системи інформаційної безпеки через формування захисних стратегій.

Частково цей підхід знаходить відображення у нормативно-правових актах. Наприклад, у Плані заходів реалізації Стратегії кібербезпеки України містяться наступні перспективні цілі: забезпечення дієвої кібероборони; ефективна протидія розвідувально-підривній діяльності у кіберпросторі; ефективна протидія кіберзлочинності; розбудова кібероробізнаного суспільства та науково-технічне забезпечення кібербезпеки; формування нової моделі відносин у сфері кібербезпеки; прагматичне міжнародне співробітництво [8]. Однак ми вважаємо, що цей підхід не є перспективним, оскільки він не враховує багато важливих аспектів, зокрема зв'язок між належним станом інформаційної безпеки та координацією зусиль влади і громадянського суспільства у цій сфері.

Таким чином сформувалося три ключові підходи до визначення пріоритетних напрямів розвитку системи забезпечення інформаційної безпеки. Коротко схарактеризує ці підходи:

– суб'єктоцентричний – в основі цього підходу є організаційно-правовий пріоритет, тобто формування особливої моделі забезпечення інформаційної безпеки через взаємодію різних за статус суб'єктів владних повноважень. В рамках цього підходу науковці акцентують увагу на розподілі означених повноважень та окресленні компетенції, розглядаючи ці категорії як основу ефективного захисту національних інтересів в інформаційній сфері;

– правоцентричний – в основі цього підходу є нормотворчість на усіх рівнях владної вертикалі. Тобто, інформаційна безпека розглядається як правова конструкція, функціонування якої визначається законодавчими і підзаконними актах. Науковці, які обгрунтовують цей підхід, надають нормативно-правовій складовій вирішальне значення та визнають її здатність до врегулювання найбільш ключових аспектів забезпечення інформаційної безпеки на усіх її рівнях;

– об'єктоцентричний – цей підхід заснований на характері і природі

самої інформації, вплив якої може бути як конструктивний так і деструктивний. Інакше кажучи, система інформаційної безпеки має формуватися на основі поділу інформації на дві означені категорії. Науковці, які підтримують цей підхід вважають, що політика держави в сфері інформаційної безпеки повинна концентруватися на протидії деструктивного впливу та сприянні поширенню об'єктивної і достовірної інформації.

Вважаємо за необхідно висловити власну думку щодо трьох окреслених підходів. Правоцентричний підхід має право на існування, оскільки кожна сфера владно-розпорядчої діяльності вимагає нормативно-правового регулювання. Не є винятком сфера національної безпеки та її інформаційна складова, яка має бути максимально формалізована. Нормативно-правове визначення окремих аспектів інформаційної безпеки дійсно має важливе значення, адже дозволяє спрямувати організаційно-розпорядчий вплив та впорядкувати діяльність усіх учасників інформаційної діяльності в державі. Також на цьому рівні можна деталізувати певні ідеологічні засади у вигляді пріоритетів, інтересів та принципів. Однак, правової регламентації не достатньо, оскільки виключна імперативність не забезпечує розвиток національної інформаційної системи. Тому, цей підхід є невід'ємним елементом цілісної моделі інформаційної безпеки України.

Об'єктоцентричний підхід також не вбачається перспективним, оскільки система інформаційної безпеки не може спиратися на розподіл інформації. Звісно, на нормативно-правовому рівні такий розподіл опосередковано присутній через візуалізацію правових режимів доступу до інформації, а також встановлення заборон щодо поширення окремих її видів. Однак, цілісна модель повинна спиратися на більш глобальні категорії, які дозволяють запобігати та протидіяти загрозам інформаційної безпеки. Недоліком цього підходу також є ризик виникнення певного конфлікту на різних рівнях інформаційної безпеки. Вони можуть бути реакцією на невідповідність національних інтересів потребам суспільства та особистості. Тому, цей підхід не може бути основою розбудови організаційно-правових засад забезпечення інформаційної безпеки.

Найбільш прийнятним є суб'єктоцентричний підхід, який спирається на поєднання зусиль різних за статусом учасників інформаційних правовідносин. Втім, цей підхід також не позбавлений недоліків. Його прихильники здебільшого міркують над розподілом повноважень та координацією дій між суб'єктами владних повноважень, нівелюючи при цьому роль громадянського суспільство. До речі, останнє обмежується консультативно-дорадчими повноваженнями, які не дозволяють ефективно захищати інтереси суспільства та особистості. Тобто, громадськість виступає у якості факультативного суб'єкта, завданням якого є дотримання встановлених державою вимог, а також часткове сприяння у виявленні порушень інформаційного законодавства та доведенні цієї інформації до правоохоронних органів. На нашу думку, такий підхід також є неконструктивним, адже суттєво обмежує громадськість в практичних можливостях реалізації і захисту права на інформацію.

На нашу думку, актуальним є четвертий підхід: розбудова моделі громадського інформаційного врядування. У наукових колах вже з'являються праці, в яких вчені міркують над новою моделлю забезпечення інформаційної безпеки. Зокрема. О. М. Солодка стверджує, що основою політики інформаційної безпеки України має стати система «суспільство – держава», а також перехід від захисних стратегій до наступальних. Дослідниця систематизує наступні засади зміцнення організаційних основ забезпечення інформаційної

безпеки: 1) вирішення питання координації діяльності суб'єктів забезпечення інформаційної безпеки; 2) налагодження системи державно-приватного партнерства у сфері забезпечення інформаційної безпеки; 3) запровадження системи демократичного контролю за діяльністю державних суб'єктів [9, с. 41]. Отже, в основі моделі громадського інформаційного врядування має бути партнерство між владою та громадянським суспільством у сфері інформаційної діяльності та забезпечення інформаційної безпеки держави, суспільства та особистості.

Висновки з дослідження і перспективи подальших розвідок у даному науковому напрямку. Підводячи підсумки зазначимо, що на сьогодні жоден з існуючих наукових підходів до визначення перспектив розвитку системи інформаційної безпеки не відповідає реаліям сучасності. Збройна агресія змушує владу шукати нестандартні рішення та делегувати частину своїх повноважень громадськості. У зв'язку з цим, перспективним вбачається громадське інформаційне врядування, яке представляє собою організаційно-правову модель забезпечення інформаційної безпеки держави, яка передбачає реалізацію особливих правових методів та форм захисту національних інтересів в інформаційній сфері на основі партнерства між державою та громадянським суспільством. Успішне запровадження вказаної моделі вимагає формування національного інформаційного простору, який представляє собою індивідуалізований національний контекст розвитку окремих видів інформаційної діяльності, розглянутий через призму загроз і викликів, а також особливості системи суб'єктів інформаційної безпеки. Формалізація цієї категорії в законодавстві дозволить поєднати інтереси держави, суспільства та особистості в інформаційній сфері в рамках єдиної системи ціннісних орієнтирів. Перспективним напрямом наукового пошуку залишається питання нормативно-правового визначення моделі громадського інформаційного врядування.

У статті досліджено проблемні аспекти визначення перспектив розвитку системи інформаційної безпеки України. Автор проаналізував три підходи до визначення пріоритетних напрямів розвитку системи забезпечення інформаційної безпеки. Було встановлено, що в основі суб'єктоцентричного підходу є формування особливої моделі забезпечення інформаційної безпеки через взаємодію різних за статус суб'єктів владних повноважень. Автору вдалося з'ясувати, що правоцентричний підхід грунтується на нормативно-правовій складовій, яка визначає ключові аспекти забезпечення інформаційної безпеки на усіх її рівнях. Встановлено, що об'єктоцентричний підхід заснований на характері і природі самої інформації, вплив якої може бути як конструктивний так і деструктивний. Наголошено, що жоден з існуючих наукових підходів до визначення перспектив розвитку системи інформаційної безпеки не відповідає реаліям сьогодення. У зв'язку з цим, автор обґрунтовує необхідність розбудови громадського інформаційного врядування, яке представляє собою організаційно-правову модель забезпечення інформаційної безпеки держави, що передбачає реалізацію особливих правових методів та форм захисту національних інтересів в інформаційній сфері на основі партнерства між державою та громадянським суспільством. Увага також приділяється проблемі формування національного інформаційного простору, який представляє собою індивідуалізований національний контекст розвитку окремих видів інформаційної діяльності, розглянутий через призму загроз і викликів, а також особливості системи суб'єктів інформаційної безпеки.

Ключові слова: громадське інформаційне врядування, захист інформації, інформаційна безпека, інформаційна діяльність, національний інформаційний простір, право на інформацію.

Nedokhlebov I. I. Problems of determining prospective directions of development of the information security system of Ukraine

The article examines the problematic aspects of determining the prospects for the development of the information security system of Ukraine. The author analyzed three approaches to determining the priority areas of development of the information security system. It was established that the basis of the subject-centric approach is the formation of a special model of ensuring information security through the interaction of authorities with different statuses. The author was able to find out that the right-centered approach is based on the normative-legal component, which determines the key aspects of ensuring information security at all its levels. It was established that the object-centric approach is based on the character and nature of the information itself, the influence of which can be both constructive and destructive. It is emphasized that none of the existing scientific approaches to determining the prospects for the development of the information security system correspond to the realities of today. In this regard, the author substantiates the need for the development of public information governance, which is an organizational and legal model for ensuring the information security of the state, which involves the implementation of special legal methods and forms of protection of national interests in the information sphere based on a partnership between the state and civil society. Attention is also paid to the problem of the formation of the national information space, which is an individualized national context of the development of certain types of information activities, considered through the prism of threats and challenges, as well as the peculiarities of the system of information security subjects.

Key words: public information governance, information protection, information security, information activity, national information space, right to information.

Література

1. Троянський О. А. Інформаційна безпека України: сучасний стан та перспективи розвитку. Науковий вісник Льотної академії. 2021. С. 185–194.

2. Крюков О. І. Інформаційна безпека держави в умовах глобалізації. Державне будівництво. 2007. № 2. С. 106–112.

3. Лисенко С. О. Сучасні тенденції розвитку інформаційної безпеки як об'єкта правовідносин. Публічне урядування. 2019. № 17. С. 154–173.

4. Басенко Р. О., Шаравара Р. І., Кравченко А. П. Перспективи розвитку правового забезпечення протидії інформаційній війні. Юридичний науковий електронний журнал. 2023. № 4. С. 28–30.

5. Про затвердження Концепції технічного захисту інформації в Україні: Постанова Кабінету Міністрів України від 08 жовтня 1997 р. № 1126. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text (дата звернення: 28.01.2024).

6. Інформаційно-аналітичні матеріали до парламентських слухань «Реформування галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України». Інститут інформаційних технологій і засобів навчання НАПН України. 2016. 15 с.

7. Федорова Н. Є., Смєсова В. Л. Інформаційна безпека та шляхи її забезпечення на етапі інформаційно-технологічної революції. Причорноморські економічні студії. 2020. № 57. С. 13–16.

8. Про План реалізації Стратегії кібербезпеки України: Рішення ради національної безпеки і оборони України від 30 грудня 2021 р. Голос України. 2022. № 21.

9. Солодка О. М. Пріоритети удосконалення інформаційної безпеки України. Інформація і право. 2015. № 3. С. 36–42.