

УДК 342.951(477)

В. В. Філатов, кандидат юридичних наук,
старший викладач кафедри цивільного,
господарського та екологічного права
Університету митної справи та фінансів

ЗАГАЛЬНА ТЕОРІЯ БЕЗПЕКИ ЯК МЕТОДОЛОГІЧНА ЗАСАДА ДОСЛІДЖЕННЯ КАТЕГОРІЇ “ІНФОРМАЦІЙНА БЕЗПЕКА”

Визначено місце та роль загальної теорії безпеки в методології дослідження категорії “інформаційна безпека”. Окреслено перспективні напрями наукового опрацювання питань інформаційної безпеки. Охарактеризовано інші складники методології дослідження інформаційної безпеки держави, суспільства та особи.

Ключові слова: інформаційна безпека; методологія; загальна теорія безпеки; інтереси держави в інформаційній сфері; дослідження.

The article defines the place and role of the general theory of security in the methodology of the research category “information security”. Ensuring national security is one of the main priorities at the present stage of Ukraine’s development. The challenges facing the state today requires detailed scientific elaboration of individual components of national security. It should be noted that the legislation in this area is sufficiently branched, which negatively affects the mechanisms of prevention and localization of internal and external threats to the sovereignty and territorial integrity of the state. This also applies to such an element as the information security of Ukraine, since it is possible to observe not only the gaps in the legislation, but also the absence of complex scientific works, which reveals the content, the essence of the functional purpose of this component of national security. As a result, the information sphere remains rather vulnerable, and the level of protection of the interests of the state – it is necessary low. The purpose of the paper is in the detailed theoretical and legal analysis of the general theory of security as the main methodological basis for the study of the category of “information security”. Perspective directions of scientific research of information security issues are outlined. Among such areas are: the scientific elaboration of a range of state interests in the information sphere; selection and analysis of individual levels of information security (security of the state, society and person); development of criteria for the effectiveness of information security policies; coordination of the directions of administrative reform with the priorities of information security; the decision of the sphere of application of foreign experience in the field of information security. Other components of the methodology of information security research of the state, society and person are briefly described, in particular a set of general law and special methods used in administrative law.

Key words: information security; methodology; salary theory of security; interests of the state in the information sphere; research.

Постановка проблеми. Забезпечення національної безпеки – один з основних пріоритетів на сучасному етапі розвитку України. Виклики, які нині постали

© В. В. Філатов, 2017

перед державою, потребують детального наукового опрацювання окремих складників національної безпеки. Слід зазначити, що законодавство у цій сфері достатньо розгалужене, що негативно позначається на механізмах запобігання та локалізації внутрішніх і зовнішніх загроз суверенітету та територіальній цілісності держави. Це стосується такого складника, як інформаційна безпека України, адже можна спостерігати не тільки прогалини у законодавстві, але й відсутність комплексних наукових праць, у яких розкривається зміст, сутність і функціональне призначення цієї складової частини національної безпеки. Як наслідок, інформаційна сфера залишається досить вразливою, а рівень захищеності інтересів держави дуже низьким.

Аналіз останніх досліджень і публікацій. У вітчизняній юридичній науці питання методології дослідження правових явищ у різні часи аналізували О. Бригінець, І. Жаровська, О. Крупчан, Ю. Лісовська, В. Пасічник, В. Шейко та інші науковці. Однак в умовах оновлення законодавства про інформаційну безпеку та появи нових загроз в інформаційній сфері з'явилася необхідність комплексного наукового осмислення і пошуку нових підходів щодо його вирішення. Необхідно переглянути методологічну основу дослідження, зокрема проаналізувати місце у цій методології загальної теорії безпеки.

Постановка проблеми. В структурі національної безпеки України інформаційна безпека – найменш формалізована категорія, яка донедавна взагалі не виділялась як окремий складник. Положення чинного законодавства та підзаконні акти не враховують усієї специфіки інформаційної сфери, мають недоліки щодо пріоритетних напрямів діяльності влади у запобіганні внутрішнім і зовнішнім загрозам. У таких умовах потрібне детальне наукове опрацювання методологічних засад дослідження інформаційної безпеки, зокрема загальної теорії безпеки.

Мета статті полягає у детальному теоретико-правовому аналізі загальної теорії безпеки як основної методологічної засади дослідження категорії “інформаційна безпека”.

Виклад основного матеріалу. Дослідження будь-якої правової категорії потребує попереднього визначення методологічних засад, які дають змогу у подальшому всебічно та об'єктивно розглянути предмет наукового пошуку. В. М. Шейко вважає, що методологія дослідження правових явищ:

- 1) визначає способи здобуття наукових знань, які відображають динамічні процеси та явища;
- 2) спрямовує дослідника на особливий шлях, на якому досягається певна науково-дослідна мета;
- 3) забезпечує всебічність і повноту отримання інформації, необхідної для пізнання процесу чи явища, що вивчається;
- 4) сприяє поповненню новою інформацією фонду теорії науки;
- 5) допомагає в уточненні, збагаченні, систематизації термінів і понять у науці;
- 6) створює систему наукової інформації, що ґрунтується на об'єктивних фактах;
- 7) логіко-аналітичний інструмент наукового пізнання [1, 56].

Слід додати, що методологічні засади також дають можливість визначити природу досліджуваного явища, яка так чи інакше пов'язана із уже відомими категоріями (передусім філософськими).

На підтвердження цього слід навести тезу І. М. Жаровської, яка стверджує, що методологія правознавства – це складне, багатопланове утворення, яке охоплює проб-

леми структури юридичного наукового знання загалом і особливо його теорії, концепції; тенденції виникнення, функціонування і зміни наукового знання, а також його класифікації, типології тощо; понятійний апарат методології та її наукову мову; структуру і склад методологічного підходу та інших наукових методів, що застосовуються в юридичній науці; формалізовані методики і процедури конкретних юридичних досліджень. Якщо методологію юридичної науки розглядати не тільки як сукупність її методів і знань про них, а в широкому розумінні – ще як симбіоз предметних правових теорій, понять, принципів тощо, то вона за обсягом змісту наближається до всієї юридичної науки, однак у методологію ці елементи системи юридичних наукових знань входять тільки тими їхніми властивостями (сторонами), які можуть і повинні використовуватись як методи наукового пізнання [2, 138].

На нашу думку, основною методологічною засадою дослідження інформаційної безпеки є загальна теорія безпеки, яка у наукових колах обговорюється досить активно. Зокрема слід зупинитися на таких визначеннях науковців:

– безпека – самостійна галузь правової охорони і захисту конституційних та інших законних інтересів особи, суспільства, держави і нації, котра обумовлена такими, що створюють високу ймовірність завдання шкоди цим інтересам, фізичними, хімічними і біологічними проявами та діями природного середовища і технічних систем, пов'язаними з правопорушеннями та юридичними казусами, а також такими, що підлягають офіційній оцінці з боку держави, діями фізичних і юридичних осіб із використанням предметів, явищ і процесів (техногенних і природних джерел небезпеки конституційним та іншим законним інтересам особи, суспільства, держави і нації) [3, 38];

– безпека – це такий стан захищеності буття, цінностей та інтересів суб'єкта (об'єкта) безпеки від загроз та небезпек, за якого забезпечуються оптимальні умови його життєдіяльності, розвитку та самореалізації [4];

– безпека являє собою стійку спроможність держави до швидкого протистояння ризикам і загрозам. Це здатність стратегічно-тактичного прогнозування параметрів розвитку середовища на перспективу, що формує базову основу для забезпечення ефективної підтримки позитивних процесів у державі [5, 41].

Із вищенаведеного можна зробити висновок, що безпека – це передусім стан захищеності, який характеризується мінімальними ризиками стороннього впливу (зовнішнього або внутрішнього). З огляду на це безпека може розглядатись як явище суспільно-правове, оскільки її основне функціональне призначення пов'язане зі створенням відповідних умов суспільного життя, коли індивіду нічого не загрожує. До того ж слід припустити, що безпека як правовий феномен логічно пов'язана з небезпекою, яка й визначає сенс її існування. Тобто безпека – своєрідний індикатор неможливості виникнення загроз, хоча теоретично такий стан нереальний, адже динамічний розвиток суспільства обумовлює появу нових загроз, які протягом певного періоду часу мають негативний вплив. Відтак безпека характеризується певною ілюзорністю, адже вона існує до моменту виникнення нової загрози.

Для досліджуваної сфери така ілюзорність дуже актуальна тому, що розвиток інформаційно-телекомунікаційних технологій, як правило, випереджає розвиток відповідних методів та форм їхнього законодавчого унормування. Слід визнати, що вже давно інформація стала засобом впливу на владу, суспільство, свідомість звичайних громадян. Інформаційний тероризм, пропаганда, незаконне обмеження дос-

тупу до інформації, шпionаж за допомогою інформаційних технологій – ось лише деякі приклади маніпулювання за допомогою інформації. У зв'язку із цим методологія дослідження інформаційної безпеки повинна вважатися не тільки основою наукових пошуків у цій сфері, але й фундаментом формування інформаційної політики держави та політики національної безпеки.

Загальна теорія безпеки вказує на декілька принципових напрямів такої роботи:

– необхідно чітко проаналізувати коло інтересів держави в інформаційній сфері (мається на увазі безпековий вимір). Нині повний перелік таких інтересів наведено в Доктрині інформаційної безпеки України, затвердженій відповідним Указом Президента України від 25 лютого 2017 р. № 47/2017. До них зараховано: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; захищеність від руйнівних інформаційно-психологічних впливів; захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації; всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності в доступі до достовірної та об'єктивної інформації; розвиток та захист національної інформаційної інфраструктури; розвиток медіакультури суспільства та соціально відповідального медіасередовища; формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів; безпечне функціонування і розвиток національного інформаційного простору та його інтеграція в європейський і світовий інформаційний простір; розвиток системи стратегічних комунікацій України; захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлено законом, тощо [6]. Кожен із вищезазначених інтересів потребує додаткового наукового обґрунтування, зокрема слід зосередитися на питаннях механізмів їхнього захисту;

– необхідно виділяти й окремо досліджувати інформаційну безпеку держави, суспільства та особи. Така індивідуалізація необхідна, оскільки на кожному із зазначених структурних рівнів інформаційної безпеки існують свої внутрішні та зовнішні загрози. Вони достатньо специфічні та потребують окремого наукового аналізу. Однак при цьому слід пам'ятати, що лише сукупність цих складників забезпечує максимальний рівень захисту інформаційного простору України. Це свідчить на користь взаємообумовленості та взаємозв'язку між цими структурними рівнями, які слід урахувати в розробці напрямів інформаційної політики держави. До речі, залежно від рівня визначаються не тільки загрози, але й засоби запобігання їм та локалізації наслідків;

– необхідно детально аналізувати пріоритети інформаційної безпеки, тобто зосереджуватися на кінцевому результаті, який досягається за допомогою комплексу методів і форм. У цьому сенсі доцільно звернути увагу на критерії ефективності політики держави у сфері інформаційної безпеки. Це дуже важливий показник, адже він відображає відповідність витрачених ресурсів меті виконавчо-розпорядчої діяльності у сфері інформаційної безпеки. Передусім ці питання мають бути формалізовані в Законі України “Про основи національної безпеки України” від 19 червня 2003 р. № 964-IV, в якому інформаційна безпека позиціонується як окрема самостійна складова частина [7];

– необхідно вирішити питання суб'єктів, які відповідатимуть за реалізацію політики інформаційної безпеки. Окремо слід сконцентруватися на їхньому право-

вому статусі, створенні оптимальної моделі управління інформаційною безпекою, яка відповідатиме напрямам адміністративної реформи. Зокрема йдеться про такі напрями: створення нової правової бази, що регламентуватиме державне управління в Україні; формування нових інститутів, організаційних структур та інструментів здійснення державного управління; кадрове забезпечення нової системи державного управління; зміцнення та формування нових фінансово-економічних основ функціонування державного управління; формування механізмів наукового та інформаційного моніторингу функціонування системи державного управління [8]. При цьому слід розглянути питання впливу політики інформаційної безпеки на саму адміністративну реформу, тобто проаналізувати потребу трансформації вищезазначених напрямів та пристосування їх до пріоритетів Доктрини інформаційної безпеки України;

– необхідно розглянути можливість застосування позитивного зарубіжного досвіду у сфері забезпечення інформаційної безпеки в Україні. Як стверджує Ю. П. Лісовська, розв'язання проблем інформаційної безпеки в межах Європейського Союзу передбачає: створення спільної стратегії європейської інформаційної безпеки, протидії кібервійні, інформаційному тероризму і боротьбі з інформаційною злочинністю. При цьому вступ України до Ради Європи, членство в Європейській телерадіомовній спілці полегшують її входження в європейський і водночас світовий масово-комунікаційний простір, створюють нові можливості для укладання міждержавних угод із сусідніми країнами, а також дають змогу поглиблювати кооперацію і співпрацю між європейськими та вітчизняними масово-комунікаційними системами [9, 14]. Однак, на нашу думку, слід урахувати і деякі застереження щодо співпраці у сфері інформаційної безпеки, зокрема: необхідно використовувати лише позитивний досвід; не слід поширювати відомості про наявні та потенційні загрози інформаційній безпеці; не допускати європейських партнерів до інформації з обмеженим доступом та державної таємниці.

Окрім теорії безпеки, методологічною основою дослідження проблем інформаційної безпеки слід вважати: рівень загальнометодологічних основ (сукупність універсальних наукових принципів та понять), рівень теоретичних знань (система конкретних адміністративно-правових методів), рівень спеціально-методологічних основ (спеціальні методологічні прийоми та засоби пізнання). При чому доцільно окремо аналізувати структуру побудови системи інформаційної безпеки, процеси функціонування даної системи, напрями її розвитку й удосконалення [10, 25]. Така комплексна методологія забезпечить усебічність та об'єктивність дослідження категорії “інформаційна безпека”, що у подальшому допоможе напрацювати ефективні напрями відповідної державної політики.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. На сучасному етапі розвитку України питання інформаційної безпеки достатньо актуальні для держави та суспільства. Аналіз положень загальної теорії безпеки дає змогу визначити напрями дослідження інформаційної безпеки, а саме:

- наукове опрацювання кола інтересів держави в інформаційній сфері;
- виділення та аналіз окремих рівнів інформаційної безпеки (безпека держави, суспільства та особи);
- розробка критеріїв ефективності політики інформаційної безпеки;

– узгодження напрямів адміністративної реформи з пріоритетами інформаційної безпеки;

– використання сфер застосування зарубіжного досвіду у сфері інформаційної безпеки. Окрім загальної теорії безпеки, складником методології дослідження інформаційної безпеки є сукупність загальноправових та спеціальних методів, що застосовуються у сфері адміністративного права. При цьому перспективним напрямом подальшого наукового пошуку в цій сфері є детальний розгляд функціонального призначення цих методів щодо аналізу окремих питань категорії “інформаційна безпека”.

Список використаних джерел:

1. Шейко В. М. Організація та методика науково-дослідницької діяльності : підручник / Шейко В. М. – К. : Знання, 2006. – 308 с.
2. Жаровська І. М. Щодо проблеми методології теорії держави і права [Електронний ресурс] / І. М. Жаровська // Вісник Національного університету “Львівська політехніка”. Юридичні науки. – 2015. – № 827. – С. 138–141. – Режим доступу : http://nbuv.gov.ua/UJRN/vnulpurn_2015_827_24
3. Подоляка С. А. Безпека як складова правової системи України [Електронний ресурс] / С. А. Подоляка // Наше право. – 2015. – № 1. – С. 34–38. – Режим доступу : http://nbuv.gov.ua/UJRN/Nashp_2015_1_8
4. Пасічник В. М. Філософська категорія безпеки як основа нової парадигми державного управління національною безпекою [Електронний ресурс] / В. М. Пасічник // Демократичне врядування. – 2011. – Вип. 7. – Режим доступу : http://www.nbuv.gov.ua/UJRN/DeVr_2011_7_7
5. Бригінець О. О. Правове забезпечення фінансової безпеки України : дис. ... д-ра юрид. наук : 12.00.07 / Олександр Олексійович Бригінець ; Університет Державної фіскальної служби України. – Ірпінь, 2017. – 464 с.
6. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. “Про Доктрину інформаційної безпеки України” : Указ Президента України від 25 лютого 2017 р. № 47/2017 // Урядовий кур’єр. – 2017. – № 38.
7. Про основи національної безпеки України : Закон України від 19 червня 2003 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 38. – Ст. 351.
8. Про заходи щодо впровадження Концепції адміністративної реформи в Україні : Указ Президента України від 22 липня 1998 р. № 810/98 // Офіційний вісник України. – 1999. – № 21. – С. 32. – С. 943.
9. Лісовська Ю. П. Адміністративно-правове забезпечення інформаційної безпеки в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 “Адміністративно-правове забезпечення інформаційної безпеки в Україні” / Юлія Петрівна Лісовська. – К., 2017. – 19 с.
10. Крупчан О. Методологія досліджень діяльності органів виконавчої влади в науці адміністративного права [Електронний ресурс] / О. Крупчан // Теорія і практика інтелектуальної власності. – 2013. – № 4. – С. 68–73. – Режим доступу : http://www.nbuv.gov.ua/UJRN/Tpio_2013_4_10