information in countries such as the USA, Germany, the United Korolivstvayi, France, Hungary, Sweden, Czech Republic and other EU countries. Systemized permissible restrictions on freedom of public information, which are used in international practice and further use require detailed legal justification. It was established that the national legislation of many countries have common regulations (generally laws) that govern the right of citizens to information, but most of them related to access to information that is held by public authorities. Proved that international experience shows that the process of access to public information on its carrier (the owner) to the user can be both directly and through information intermediaries.

The role of the mediator often perform media. Determined that in general international practice of countries have adopted laws on access to public information, evidence of the positive impact of legislative changes on the implementation of the citizens fundamental rights, improve the efficiency of government and reducing the risk of corruption in the informative sphere.

Key words: *international experience, public information, access to information regulations, legislation.*

Стаття надійшла 18 травня 2016 р.

УДК 342.727:007

О. Г. Ярема,
С. С. Єсімов

ПРЕДМЕТ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНОМУ ПРАВІ

Розглянуто проблеми визначення предмета правового забезпечення інформаційної безпеки в інформаційному праві у контексті дослідження правовідносин, пов'язаних із забезпеченням стану захищеності найзначущіших інтересів особистості, суспільства та держави в інформаційній сфері від внутрішніх і зовнішніх загроз. Обґрунтовано доцільність прийняття закону «Про інформаційну безпеку» в умовах адаптації національного законодавства до вимог Європейського Союзу.

Ключові слова: *інформаційне право, предмет правового регулювання, правові відносини.*

Постановка проблеми. Дослідження предмета інформаційного права суспільних відносин у сфері використання засобів обробки та передачі інформації зумовлено розвитком нових технологій, які сприяють змінам у політичній, соціально-економічній та інших сферах суспільного життя. Однак досягнення технічного прогресу має не тільки

переваги, а й є передумовою для виникнення загроз, що вимагають адекватних заходів протидії з метою забезпечення захищеності життєво важливих інтересів особистості, суспільства і держави в інформаційній сфері. У науковій літературі зауважено, що в умовах розвитку інформаційного суспільства змінюється вияв деяких ознак держави: в інформаційному просторі немає територіальних меж, що призводить до проблем правового характеру щодо суверенітету, юрисдикції, колізій національних законодавств. Географічні межі трансформуються в електронні кордони, що вимагає уваги до проблематики інформаційної безпеки [1, с. 181]. Це особливо виявляється в умовах агресії Російської Федерації стосовно України.

Стан дослідження. Окремі успішні спроби аналізу структури інформаційного законодавства були, наприклад, у роботах учених у галузі інформаційного права (В. М. Брижко, В. Д. Гавловський, М. З. Згуровський, М. К. Родіонов, І. Б. Жиляєв, Р. А. Калюжний, Л. П. Коваленко, Б. А. Кормич, Т. А. Костецька, А. М. Кузьменко, М. Я. Швець тощо), в яких інституційний розвиток інформаційного законодавства, визначення місця правового забезпечення інформаційної безпеки трактується як наукове завдання інформаційного права. Проте досі вона залишається невирішеною, як і не сформовано єдиного підходу до визначення структури системи правового забезпечення інформаційної безпеки.

Метою статті є аналіз інституційного розвитку правового забезпечення інформаційної безпеки.

Виклад основних положень. Чинники і тенденції розвитку сучасного суспільства (створення обчислювальної техніки, використання високих технологій обробки та передачі інформації, масова інформатизація) змінили характеристику інформації та пов'язаної з нею інфраструктури, наділили їх властивостями, які формують систему суспільних відносин. Характерними ознаками інформаційної сфери та відносин, що в ній сформувалися, є підвищена актуальність, складність, недостатня структурованість їх об'єкта та невизначений стан суб'єктного складу, висока швидкість зміни й оновлення технологій обробки та передачі інформації, труднощі в жорсткій фіксації юридичних фактів і складів у віртуальному інформаційному середовищі, неоднорідність предмета правового регулювання.

Структурування правового забезпечення інформаційної безпеки в системі національного права обумовлено наявністю специфічних чинників, які пов'язані з розвитком інформаційних технологій, становленням в Україні інформаційного суспільства, зростанням цінності інформаційних ресурсів, формуванням нового типу відносин – інфор-

маційних, а також виникненням загроз інформаційним інтересам особистості, суспільства і держави. Вивчення вказаних обставин дає змогу стверджувати, що в основі формування структурного утворення в системі права, спрямованого на забезпечення правового захисту інтересів суб'єктів інформаційної сфери, є об'єктивні чинники:

– тенденції розвитку інформаційного суспільства, заснованого на масовому застосуванні інформаційних технологій, зростанні економічної та соціальної значущості інформації. В суспільстві виник специфічний вид правовідносин – інформаційні відносини, що формуються з приводу споживання благ інформаційного характеру та потребують правового регулювання. Однак поряд із появою інформаційних благ формується тенденція до збільшення конфліктів інтересів із приводу інформаційних ресурсів, загострюються суперечності між учасниками інформаційних процесів, виникають загрози життєво важливим інтересам особистості, суспільства та держави. Відповідно, з'являється потреба в захисті від загроз життєво важливих інтересів особистості, суспільства та держави, забезпеченні їхньої безпеки;

– відокремлення предмета правового регулювання – відносин, пов'язаних із забезпеченням захищеності найзначущіших інтересів особистості, суспільства та держави в інформаційній сфері від внутрішніх і зовнішніх загроз. Ці відносини є різновидом інформаційних правовідносин, що виникають у процесі діяльності щодо забезпечення інформаційної безпеки;

– чинники теоретико-методологічного характеру, що визначають тенденцію потреби з боку суспільства розвитку правової науки в галузі правового забезпечення інформаційної безпеки, що відображено в роботах українських учених, які обґрунтовують наявність галузі інформаційного права та його елементів, зокрема правове забезпечення інформаційної безпеки.

Указані чинники взаємопов'язані та розглядаються як стійкі тенденції інституційного типу, а формування підгалузі правового забезпечення інформаційної безпеки має закономірний характер.

Законодавство про інформаційну безпеку входить у систему інформаційного законодавства та регулює відносини у вказаній сфері. Розвиток національного законодавства у зазначеній сфері розпочався після прийняття 1994 року Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», хоча термін «інформаційна безпека» введено Указом Президента України від 23.04.2008 № 377/2008 «Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року «Про невідкладні заходи щодо забезпечення інформаційної безпеки України»» [2; 3].

Необхідність адаптації національного законодавства до вимог Європейського Союзу зумовлює інтенсивний розвиток інформаційного законодавства, зокрема про інформаційну безпеку, за різними напрямами (прийняті закони України «Про захист персональних даних», «Про електронний цифровий підпис», «Про внесення змін до деяких законодавчих актів України щодо інсайдерської інформації» тощо [4]). Водночас доцільно зауважити на неврегульованість відносин щодо забезпечення інформаційної безпеки в різних сферах життя суспільства. Відсутність нормативного визначення низки термінів («інформаційна безпека», «службова таємниця», «інформаційний екстремізм» та ін.) призводять до дефектів законодавства про інформаційну безпеку, що, на нашу думку, спричинено недостатньою структурною сформованістю правового забезпечення інформаційної безпеки. З огляду на це є доцільним реформування законодавства у сфері забезпечення інформаційної безпеки. Це повинно охоплювати систематизацію чинних законів, законодавче закріплення визначень низки термінів, принципів, засад державної політики в сфері забезпечення інформаційної безпеки, врегулювання проблем, пов'язаних із охороною службової таємниці, протидією інформаційному екстремізму, тощо. Деякі зазначені аспекти відображено у Стратегії національної безпеки України та проекті Доктрини інформаційної безпеки України [5; 6]. Водночас реформування можливе на теоретичній основі, що вимагає обґрунтування природи, структури та місця інституту правового забезпечення інформаційної безпеки в системі права.

Зважаючи на проведені дослідження комплексної природи галузі інформаційного права (Р. А. Калюжний, Б. А. Кормич, Т. А. Костецька та ін.), а також аналіз характеру та структури правовідносин, правове забезпечення інформаційної безпеки є самостійним правовим утворенням, яке є підгалуззю інформаційного права, оскільки має власну складну структуру, що охоплює інститут віднесення інформації до категорії з обмеженим доступом, інститут захисту інформації та ліцензування цієї діяльності, а також інститут відповідальності за правопорушення в інформаційній сфері.

Правове утворення, пов'язане з забезпечення інформаційної безпеки, володіє сукупністю ознак підгалузі: відокремленим предметом правового регулювання, логічно пов'язаною структурою правових режимів, комплексним використанням галузевих методів правового регулювання, а також високим ступенем спеціалізації й інтеграції правових інститутів, кожен із яких, своєю чергою, також має внутрішню структуру.

Доцільно погодитися з думкою А. М. Кузьменка, що структурна складність підгалузі пояснюється предметною безліччю правовід-

носин, що виникають під час забезпечення захищеності інтересів особистості, суспільства та держави в інформаційній сфері [7, с. 318–319].

Правовий інститут віднесення інформації до категорії з обмеженим доступом охоплює: державну, комерційну, професійну таємниці, персональні дані тощо.

У правовий інститут захисту інформації входять: правове забезпечення діяльності щодо захисту інформації та ліцензування вказаної діяльності.

Правовий інститут відповідальності за інформаційні правопорушення складається з цивільної, дисциплінарної, адміністративної та кримінальної відповідальності.

Підгалузь правового забезпечення інформаційної безпеки регулює суспільні відносини, використовуючи норми різних галузей права (водночас єдність і цілісність цих галузей не порушуються), комплексно використовуючи різні галузеві методи правового регулювання. Крім того, природа інформації як об'єкта різних суспільних відносин, врегульованих нормами різних галузей права, також має комплексний характер. Вказані особливості визначають комплексну природу цієї підгалузі. Правові норми, що входять до підгалузі, зв'язуються єдністю мети правового регулювання – забезпечення інформаційної безпеки, що виражається в стані захищеності збалансованих життєво важливих інтересів особистості, суспільства та держави.

Предмет правового регулювання – відносини, що виникають у зв'язку із забезпеченням інформаційної безпеки, охоплюють широкий спектр цих відносин, що обумовлює взаємозв'язок інституту з низкою галузей права (цивільним, адміністративним, кримінальним, конституційним).

Норми законодавства, які регулюють правовідносини, що виникають з приводу різних видів таємниці, становлять особливий конфіденційний правовий режим інформації обмеженого доступу. Відмінними ознаками правового режиму є:

– відсутність вільного доступу до інформації на законній підставі;

– невідомість інформації для третіх осіб;

– наявність законних інтересів суб'єктів у захисті цієї інформації у характерному їй режимі.

Конфіденційний правовий режим інформації обмеженого доступу охоплює режими державної, комерційної, професійної таємниці, режим персональних даних. Водночас зараз режим службової таємниці не має законодавчого закріплення, незважаючи на множинні згадки про заборону її розголошення в текстах відомчих нормативних

документів. Ця законодавча невизначеність негативно відображається на стані правового захисту інтересів суспільства та держави в інформаційній сфері. Відокремлення правового інституту віднесення інформації до категорії з обмеженим доступом обумовлене наявністю загального для всіх таємниць конфіденційного правового режиму. А відтак його інтеграція з іншими правовими інститутами логічно обумовлена зв'язком між інститутом таємниць і інститутами захисту інформації (ліцензування цієї діяльності) та відповідальністю за інформаційні правопорушення. Захист інформації, яка належить до відомостей, що становлять той чи інший вид таємниці, вимагає жорсткого державного регулювання (зокрема ліцензування) щодо її захисту, а порушення режиму таємниці та встановленого порядку провадження діяльності щодо захисту конфіденційної інформації тягне притягнення винних осіб до юридичної відповідальності. Водночас наявність зв'язку між зазначеними інститутами підтверджує обґрунтованість побудови структури підгалузі правового забезпечення інформаційної безпеки та включення до неї інституту віднесення інформації до категорії з обмеженим доступом.

Відповідно до аналізу особливостей ліцензування діяльності щодо захисту інформації стосовно особливостей застосовуваного щодо кожного з видів правового режиму (державної та комерційної таємниці, персональних даних та ін.) доцільне уточнення окремих положень чинного законодавства. Зокрема вимагає уточнення положення щодо захисту інформації, котра становить комерційну таємницю, персональних даних працівників, які обробляються на підприємстві для власних потреб, не вимагає ліцензування. Водночас для забезпечення безпеки реалізації конституційного права громадян на таємницю листування та запобігання монополізації інформаційних ринків доцільно законодавчо закріпити ліцензування діяльності з надання послуг електронної пошти.

Забезпечення інформаційної безпеки досягається комплексним застосуванням заходів дисциплінарної, адміністративної, кримінальної та цивільної відповідальності.

На думку Л. П. Коваленко, нині стан українського інформаційного суспільства потребує від правової системи динамічного розвитку, виявлення відповідних доктринальних положень і комплексної організації правового забезпечення інформаційної сфери [8, с. 126]. У вказаному контексті оптимізація законодавчого забезпечення інформаційної безпеки можлива завдяки:

– введенню несуперечливої термінології у сферу правового забезпечення, яка забезпечить дотримання основних вимог теорії права щодо однозначності;

– встановленню балансу інтересів особистості, суспільства та держави під час захисту державної таємниці, персональних даних, необхідно уніфікувати вимоги, пропоновані відомчим переліком відомостей, що становлять службову таємницю (мають гриф обмеження «для службового користування»). Це актуально з огляду на ст.ст. 25–27 Закону України «Про Національну поліцію» щодо повноважень у сфері інформаційно-аналітичного забезпечення та використання інформаційних ресурсів [9];

– скорегуванню низки повноважень Служби безпеки України у сфері захисту державної таємниці, зокрема необхідно прямо закріпити в законодавстві право Служби безпеки України на здійснення контролю за діяльністю органів місцевого самоврядування в межах цієї сфери;

– застосовуванню диференційованого підходу до вимог, які повинні встановлюватися з метою захисту комерційної таємниці її правовласником;

– приведенню Закону України «Про захист персональних даних» у відповідність до Цивільного процесуального кодексу України в частині права фізичних і юридичних осіб звертатися до суду з позовом щодо захисту прав і законних інтересів суб'єктів персональних даних і бути в суді їхнім представником.

У контексті проекту Доктрини інформаційної безпеки України доцільно з метою інституційного розвитку правового забезпечення інформаційної безпеки прийняти закон «Про інформаційну безпеку».

Закон повинен охопити: мету та сферу дії закону, основні поняття, перелік законодавчих актів, що регулюють цю сферу відносин, принципи забезпечення інформаційної безпеки, її суб'єкти та об'єкти, предмет забезпечення інформаційної безпеки у контексті юридичної науки; основні завдання правової політики в сфері, що розглядається; питання забезпечення безпеки інформації обмеженого доступу (принципи віднесення інформації до конфіденційної або секретної, види інформації обмеженого доступу); питання захисту від неправомірного впливу загальнодоступної інформації, що міститься в державних інформаційних мережах загального користування, зокрема щодо організації захисту об'єктів інтелектуальної власності; питання захисту від шкідливої та недостовірної інформації; питання протидії інформаційному екстремізму (критерії визнання інформації загрозливою конституційному ладу України); загальні умови відповідальності за інформаційні правопорушення. Закон «Про інформаційну безпеку», консолідувавши норми, які стосуються підгалузі правового забезпечення інформаційної безпеки, надалі може бути використано із метою кодифікації відомчо-

го законодавства у зазначеній сфері, зокрема щодо розробки технічних стандартів захисту інформації у зв'язку з появою нових інформаційних технологій та засобів доступу до різних інформаційних ресурсів.

Висновки. Правове забезпечення інформаційної безпеки є частиною системи інформаційного права, що обумовлено комплексною природою інформаційного права. Водночас правове забезпечення інформаційної безпеки є самостійним нормативним утворенням, що складається з системи норм інформаційного права, а також норм інших галузей права, що регулюють однорідні суспільні відносини, які виникають з приводу захисту інформації конфіденційного характеру, ліцензування діяльності щодо захисту інформації, а також установлюють відповідальність за інформаційні правопорушення. Прийняття закону «Про інформаційну безпеку» створить структурну стійкість усієї системи нормативних правових актів, що діють у вказаній сфері.

1. Emerging Electronic Highways: New Challenges for Politics and Law V. J. J. M. Bekkers, Sjaak Nouwt Kluwer Law International, 1996. – 187 p.

2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

3. Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року «Про невідкладні заходи щодо забезпечення інформаційної безпеки України»: Указ Президента України від 23.04.2008 № 377/2008 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015

4. Про внесення змін до деяких законодавчих актів України щодо інсайдерської інформації від 22.04.2011 № 3306-VI // Відомості Верховної Ради України. – 2011. – № 44. – Ст. 471.

5. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015

6. Проект Указу Президента України «Про Доктрину інформаційної безпеки України» [Електронний ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025

7. Кузьменко А. М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства / А. М. Кузьменко // Часопис Київського університету права. – 2010. – № 4. – С. 317–321.

8. Коваленко Л. П. Деякі питання щодо визначення інформаційного права / Л. П. Коваленко // Юрист України. – 2014. – № 2 (27). – С. 122–127.

9. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/main/580-19.

Ярема О. Г., Есимов С. С. Предмет правового обеспечения информационной безопасности в информационном праве

Рассмотрено проблемы определения предмета правового обеспечения информационной безопасности в информационном праве в контексте исследования правоотношений, связанных с обеспечением состояния защищенности наиболее значимых интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз.

Рассматривается целесообразность принятия закона «Об информационной безопасности» в условиях адаптации национального законодательства к требованиям Европейского Союза.

Ключевые слова: *информационное право, предмет правового регулирования, правовые отношения.*

Yarema O. H., Yesimov S. S. The subject of legal information security in information law

The research of the subject of information law of public relations in the sphere of processing and transmission of information is caused by the development of new technologies that bring changes in the political, socio-economic and other spheres of public life. However, technological progress brings not only benefits, but it is also a prerequisite for the emergence of threats that require adequate counter measures to ensure protection of vital interests of the individual, society and state in the information sphere. The scientific literature proves that in the terms of the development of the information society some characteristics of the state are changing: there are no territorial boundaries in cyberspace, and it can cause problems of a legal nature concerning the sovereignty, jurisdiction, and conflicts of the national legislation. Geographic boundaries are transforming into electronic boundaries that requires attention to issues of information security. This is particularly important problem in the conditions of Russian aggression against Ukraine.

In the context of the Information Security Doctrine Ukraine would be appropriate to adopt a law «On information security». The law should cover the purpose and scope of the basic concept, the list of legislative acts regulating this sphere of relationships, the subject of information security in the context of legal science.

Legal information security is part of information law due to the complex nature of information law. At the same time the legal information security is an independent regulatory entity, consisting of a system of rules of information law and the rules of other branches of law regulating uniform social relations that should protect information of a confidential nature, licensing and establish responsibility for information offenses. Adoption of the law «On information security» will create the structural stability of the entire system of normative legal acts.

Key words: *information law, subject of legal regulation, legal relations.*

Стаття надійшла 10 березня 2016 р.