

УДК 340.132+[351.746.1+004.9]

ДОВГАНЬ О.Д., доктор юридичних наук, старший науковий співробітник,
НДІ інформатики і права НАПрН України
ТКАЧУК Т.Ю., кандидат юридичних наук, доцент,
ННІ інформаційної безпеки НА СБ України

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ ЯК ПІДГАЛУЗЬ ІНФОРМАЦІЙНОГО ПРАВА: ТЕОРЕТИЧНИЙ ДИСКУРС

***Анотація.** У статті досліджується система правового забезпечення інформаційної безпеки держави та визначаються основні її складові. Науково обґрунтовується, що правове забезпечення інформаційної безпеки держави є підгалуззю інформаційного права.*

***Ключові слова:** інформаційна безпека, забезпечення інформаційної безпеки, національна безпека, система.*

***Summary.** The article investigates the system of legal provision of information security of the state and determines its main components. It is scientifically substantiated that the legal provision of information security of the state is a sub-branch of information law.*

***Keywords:** information security, provision of information security, national security, system.*

***Аннотация.** В статье исследуется система правового обеспечения информационной безопасности государства и определяются основные ее составляющие. Научно обосновывается, что правовое обеспечение информационной безопасности государства является подотраслью информационного права.*

***Ключевые слова:** информационная безопасность, обеспечение информационной безопасности, национальная безопасность, система.*

Постановка проблеми. В умовах інформаційної агресії з боку Росії та виникнення нових глобальних викликів у інформаційній сфері, з огляду на потребу ефективного захисту українського суспільства й держави вагомість правового забезпечення інформаційної безпеки держави, значно зростає. Слід також підкреслити, що інформаційна безпека держави є сьогодні однією із найважливіших складових національної безпеки України, значною мірою визначаючи стан захищеності, зокрема і правової, її життєво важливих інтересів. Окінавська хартія глобального інформаційного суспільства [1] також визначила правове забезпечення інформаційної безпеки одним із пріоритетів при розбудові такого суспільства.

Створення у системі права структури, пов'язаної із забезпеченням інформаційної безпеки, впливають із науково-технічного прогресу, формування суспільства інформаційного типу, проникнення інформаційних технологій в усі сфери життя, виникнення на цьому ґрунті нових викликів і загроз та потреби протидіяти їм.

Результати аналізу наукових публікацій. Проблематика системи правового забезпечення інформаційної безпеки держави у різних аспектах досліджувались у наукових працях відомих зарубіжних та вітчизняних вчених, зокрема основу цієї статті склали наукові пошуки О. Баранова, В. Брижка, Б. Герга, В. Горбуліна, С. Ларіна, Є. Мануйлова, І. Панової, В. Пилипчука, Г. Ситника, Р. Яргера та інших дослідників.

Водночас, слід констатувати, що ні в сучасній науковій літературі, ні на законодавчому рівні поки не склалося єдиного підходу до розуміння місця та ролі правового забезпечення інформаційної безпеки держави у структурі інформаційного

права. На практиці це призводить не лише до активізації наукової дискусії, але й до неадекватності розуміння змісту тих або інших положень, висновків і рекомендацій, що стосуються сфери як інформаційної безпеки України так й інформаційного права в цілому та мають прикладне значення.

Метою статті є обґрунтування інформаційної безпеки, у т.ч. її правового забезпечення, як складовою інформаційного права та галузі науки, з одного боку, а з іншого боку – як самостійна підгалузь науки, особливо в частині правового регулювання суспільних відносин, що виникають у інфраструктурній (програмно-технічній) складовій забезпечення інформаційної безпеки.

Виклад основного матеріалу. Забезпечення інформаційної безпеки – сукупність діяльності щодо недопущення шкоди властивостям об’єкта безпеки, зумовленої інформацією та інформаційною інфраструктурою, а також засобів і суб’єктів цієї діяльності. Структура цього поняття охоплює: предмет та об’єкт безпеки, загрози об’єкту безпеки, діяльність із захисту об’єкта безпеки від загроз, засоби і суб’єкти забезпечення безпеки.

Основними об’єктами інформаційної безпеки є пов’язані з національними інтересами інформація, інформаційна інфраструктура та правовий статус суб’єктів інформаційної сфери.

Суб’єктами забезпечення інформаційної безпеки є органи, організації та особи, уповноважені законом на здійснення відповідної діяльності.

Діяльність держави щодо забезпечення інформаційної безпеки, яка здійснюється в правовій формі, становить суть правового забезпечення інформаційної безпеки.

У широкому розуміння *об’єктами правового забезпечення інформаційної безпеки держави* першочергово виступає:

Особа (людина і громадянин), її права і свободи (забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних; захищеність від негативного інформаційно-психологічного впливу);

Суспільство – матеріальні і духовні цінності (збереження і примноження духовних, культурних і моральних цінностей Українського народу; забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; формування і розвиток демократичних інститутів громадянського суспільства);

Конституційний лад, суверенітет і територіальна цілісність держави (недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур; ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері; побудова та розвиток інформаційного суспільства; забезпечення економічного та науково-технологічного розвитку України; формування позитивного іміджу України; інтеграція України у світовий інформаційний простір).

Таким чином об’єктами правового забезпечення інформаційної безпеки України є: *людина і громадянин – їхні конституційні права і свободи, фізичне та психологічне здоров’я, захищеність від негативного впливу інформаційних технологій та інформації; суспільство і держава – захищеність їх законних інтересів в інформаційній сфері; інформаційні ресурси та інформаційна інфраструктура – їх цілісність, доступність та захищеність.*

Зважаючи на той факт, що об'єктами інформаційної безпеки можуть бути свідомість, психіка людей, інформаційні системи різного масштабу і різного призначення, пропонуємо об'єктом правового забезпечення інформаційної безпеки держави вважати:

- національні цінності в інформаційній сфері;
- національні інтереси в інформаційній сфері;
- національні цілі в інформаційній сфері.

Американські військові дослідники Яргер Річард та Джордж Барбер, розглядаючи дану тріаду в системі забезпечення національної безпеки держави, національні *цінності* визначають як найменш рухомий і найстабільніший елемент системи. Цінності формуються під час історичного процесу, розвитку матеріальної та духовної культури суспільства, відповідають геополітичному спрямуванню країни. Національні *інтереси* – елемент порівняно динамічний, що формується на основі національних цінностей під впливом довгострокових тенденцій суспільного розвитку. Національні *цілі* – найрухоміший елемент [2].

Доктрина інформаційної безпеки України визначає та змістовно наповнює тільки *національні інтереси* в інформаційній сфері. Відповідно до її аналізу можна виділити чотири основні складові національних інтересів України в інформаційній сфері:

Перша складова національних інтересів України в інформаційній сфері полягає в дотриманні конституційних прав і свобод людини і громадянина в області отримання інформації і користування нею, забезпеченні духовного оновлення України, збереженні і зміцненні моральних цінностей суспільства, традицій патріотизму, гуманізму, культурного і наукового потенціалу країни.

Друга складова – інформаційне забезпечення державної політики України, доведення до громадян України і міжнародної громадськості достовірної інформації про державну політику України, її офіційної позиції щодо соціально значущих подій в житті держави і міжнародного життя, із забезпеченням доступу громадян до відкритих державних інформаційних ресурсів.

Третя складова полягає в розвитку сучасних інформаційних технологій, вітчизняної індустрії інформації, в тому числі індустрії засобів інформатизації, телекомунікації і зв'язку, забезпечення потреб внутрішнього ринку її продукцією і вихід цієї продукції на світовий ринок, а також; забезпеченні накопичення, зберігання і використання вітчизняних інформаційних ресурсів. У сучасних умовах тільки на цій основі можна вирішувати проблеми створення наукоміських технологій, технологічного переозброєння промисловості, збільшення досягнень вітчизняної науки і техніки. Держава повинна зайняти гідне місце серед світових лідерів мікроелектронної і комп'ютерної промисловості.

Четверта складова передбачає захист інформаційних ресурсів від технічних розвідок, несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем.

Таким чином, реалізація визначених в Доктрині інформаційної безпеки України національних інтересів в інформаційній сфері буде ефективною і дієвою за умови законодавчого визначення *національних цінностей*, які зумовлюють потребу у розробці національних (державних) інтересів. Разом вони формують *національні цілі* (схематично це зображено на Рис. 1).

Таким чином, першочергового законодавчого визначення потребують саме національні цінності в інформаційній сфері. Дана тріада повинна бути чіткими орієнтирами формування та розвитку державної політики.

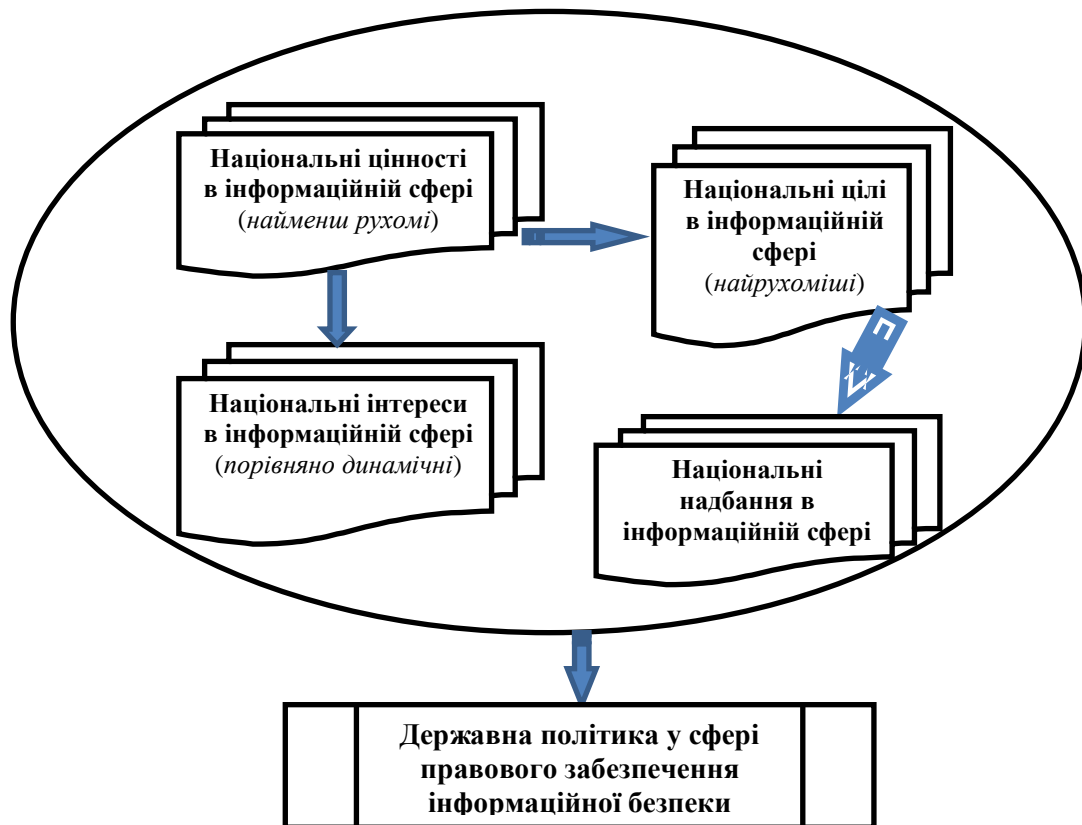


Рис. 1. Порядок взаємодії національних цінностей, інтересів, цілей та надбань в інформаційній сфері

Ми цілком підтримуємо думку Є. Мануйлова, що в стратегічному плані державі варто зміцнювати аксіосферу суспільства шляхом відтворення цінностей через освіту та виховання, дбати про інформаційну безпеку та захищеність культурно-інформаційного поля країни від зовнішніх впливів. Інформаційна стабільність та втілення чітких ціннісних пріоритетів демократичного розвитку держави забезпечуватиме її конкурентоспроможність у глобальних процесах сучасності [3, с. 16].

До цього твердження слід додати важливу засторогу відомого соціолога М. Вебера про те, що у кожній історичній епохи є своя система цінностей, тобто це категорія принципово історична [4, с. 64].

Варто погодитися з думкою С. Ларіна, що національні цінності є певними концептуальними, ідеологічними основами, консолідуючими чинниками, важливими життєвими орієнтирами на шляху ефективного суспільного розвитку [5, с. 47].

Досить ґрунтовно проблему національних цінностей досліджували вітчизняні дослідники В. Горбулін та А. Качинський. Вони структурували систему національних цінностей, поділяючи їх на цінності індивіда, цінності суспільства та цінності держави [6, с. 107]. На думку дослідників, подальше існування держави й нації має розглядатися крізь призму її ціннісного ядра, що консолідує суспільство, а саме: національна безпека, духовні надбання, добробут, система міжнародних зв'язків, патріотизм і соціальна справедливість. На нашу думку, до вищевизначеної системи національних цінностей варто також долучити такі індивідуальні цінності, як: моральність; релігійність; взаємостерпимість; миролюбність; доброзичливість; працелюбство; сім'я (сімейні цінності) тощо, які завжди були притаманними українцям і відображають сутнісні засади українського національного характеру. В. Горбулін особливо наголошував на

важливості національних цінностей, зазначаючи, що стратегія національної безпеки України формується на основі оцінок національних цінностей у контексті міжнародної обстановки [7, с. 5]. Така засторога особливо актуалізувалася з початком збройної агресії Росії проти України.

Національні цінності в інформаційній сфері – це сукупність духовних та матеріальних цінностей людини, суспільства і держави, яким властиві чітко окреслені світоглядні, соціокультурні, соціально-економічні, географічні та демографічні ознаки. Вони формують правову, філософську та етичну основу для забезпечення подальшого існування суспільства і держави, дають змогу усвідомити національну мету держави в інформаційній сфері. Національні цінності в інформаційній сфері, виходячи із сутнісного їх тлумачення, являють собою найбільш особливий сегмент, той який потребує особливого захисту. До *національних цінностей в інформаційній сфері*, з огляду на сучасний стан державотворення в Україні, слід віднести:

- *матеріальний добробут* населення, у тому числі й на основі розвитку ІКТ;
- *інформаційна захищеність* людини, суспільства, держави;
- *духовність* (доступність віросповідання, відсутність загроз, попередження релігійного фанатизму та екстремізму, недопустимість використання релігії як психологічного чинника у тероризмі, розвиток традиційних українських релігійних напрямів);
- *мова*, як основний ідентифікатор нації, як спосіб передачі інформації та знань, як пам'ять поколінь;
- *культура* інформаційних відносин;
- *свобода інформації* (захищеність інформаційних прав людини, доступ до інформації, нейтралізація негативних інформаційних впливів).

Первинним у структурі національних цінностей в інформаційній сфері має стати соціально-економічна складова інформаційної безпеки. Таким чином, на наше глибоке переконання, добробут населення, як базова категорія економічної політики держави, має стати базовим компонентом й інформаційної безпеки держави, а особливо, національної безпеки нашої держави.

На думку Г. Ситника, об'єктивне існування і вплив на безпеку особи, суспільства, держави та людської цивілізації природних і суспільних явищ зумовлює можливість розподілу цінностей на природні й соціальні [8, с. 123], що загалом й відображено у запропонованому вище переліку національних цінностей в інформаційній сфері.

Відомий вчений у галузі філософії та національної безпеки Б. Парахонський ще на початку 90-х років минулого століття зазначав, що у сучасному світі захист національних інтересів уже не може спиратися лише на стратегію силового протистояння. Ефективнішою стає реалізація власних національних інтересів за допомогою економічної, духовно-інтелектуальної експансії [9, с. 3]. Дане твердження підтверджене вітчизняною історією останнього десятиріччя зі своєю кульмінацією у 2014 році.

Таким чином, до *національних цілей в інформаційній сфері* відносимо:

покінути з порушенням та спотворенням поглядів людей на навколишній світ і самих себе, що здійснюється шляхом культивування уявних цінностей, насадження деструктивних пріоритетів, завдань і цілей перед суспільством і окремою особистістю (духовна безпека);

забезпечити впровадження інформаційних технологій у військову сферу та забезпечити їх захист (військова безпека);

прискорити розробку та впровадження новітніх конкурентоспроможних ІКТ в суспільно-економічну сферу (економічна безпека);

досягти належного рівня культури інформаційних відносин (соціальна безпека);
створити загальнодержавні інформаційні системи для постійного екологічного моніторингу стану навколишнього середовища (економічна безпека);
сприяти інтеграції національної інформаційної інфраструктури із світовою інфраструктурою.

зміцнити захист інформаційних прав людини;

вжити термінових заходів для створення позитивного іміджу держави в умовах інформаційної глобалізації.

Дещо цікавою та привабливою виступає категорія “національні надбання”, яка більш характерна для сфери культури і мистецтва. Проте, з огляду на шалений розвиток інформаційних технологій, їх визначальний вплив як на військову сферу так і на інші суспільні відносини, в першу чергу медицину, економіку, ряд здобутків інформаційної сфери поправу можна віднести до національних надбань в інформаційній сфері. При цьому, в означеній сфері вони будуть відігравати роль певного індикатора та критерію ефективності реалізації національних цілей в інформаційній сфері.

Автори законопроекту “Про інформаційну безпеку України” визначили національні надбання в інформаційній сфері як найбільш вагому, вартісну частину інформаційних ресурсів, особливо кінцеві результати інтелектуальної, творчої діяльності, кращі зразки вітчизняного (національного) інформаційного продукту без позбавлення права власності на них можуть оголошуватись національним надбанням України і незалежно від форм власності охоронятись державою як пам’ятки історії та культури. Не зовсім зрозуміло, чому автори даного законопроекту обмежилися тільки пам’ятками історії і культури, адже ці надбання мають набагато ширший спектр ціннісних орієнтирів.

На нашу думку, *національні надбання в інформаційній сфері* – це сукупність унікальних інформаційних продуктів, що мають виняткове військове, суспільне, економічне тощо значення для реалізації національних цілей в інформаційній сфері.

Створити вичерпний перелік національних надбань в інформаційній сфері не можливо, адже з кожним днем такий перелік може поповнюватися відповідними розробками чи навпаки їх виключенням у зв’язку із застарілістю чи втратою цінності. Визначальним критерієм віднесення до такого переліку є особливе, стратегічне значення інформаційного продукту як для забезпечення інформаційної безпеки держави безпосередньо, так і для розвитку інших сфер і є унікальним за своєю природою. Їх розвиток та позитивний вплив як на забезпечення інформаційної безпеки держави так і на інші дотичні сфери у значній мірі залежить від продуманої державної політики та ефективних правових механізмів її реалізації.

Варто підтримати позицію відомого українського дослідника з державного управління національною безпекою Г. Ситника, який дійшов висновку, що національні цінності визначають сутність (зміст), цілісність і стійкість, національні інтереси – структуру і характер, а національні цілі – конфігурацію та спрямованість формування та функціонування даної системи [8, с. 46]. Це стосується в цілому й інформаційної безпеки держави.

Що стосується *предмету правового забезпечення інформаційної безпеки*, то це сфера правового впливу на поведінку людей, що має на меті недопущення прояву загроз об’єктам інформаційної безпеки або мінімізацію негативних наслідків прояву цих загроз. Цю сферу утворюють сукупно суспільні відносини, що мають такі основні ознаки:

- належність до інформаційних відносин або зумовленість ними;
- зв’язок з об’єктами національних інтересів в інформаційній сфері;

- зумовленість проявів загроз безпеці об'єктам національних інтересів в інформаційній сфері.

Предметна спрямованість діяльності щодо забезпечення інформаційної безпеки визначається сукупністю суспільних відносин, пов'язаних з інформацією та інформаційною інфраструктурою у різних сферах життєдіяльності суспільства і державного управління, реалізацією правового статусу суб'єктів інформаційної сфери, проявами загроз, що здатні завдати шкоди національним інтересам.

Звертаючись до питання структурування правового забезпечення інформаційної безпеки, слід насамперед зазначити, що йдеться про формування та розвиток у системі права певного структурного утворення, яке це забезпечення регулює. А передумовами цього є чинники й тенденції не лише самої сфери інформаційних інтересів та їх захисту (предмета вказаного забезпечення), але й формування комплексних галузей законодавства та загалом системи права, а також методологічних здобутків юридичної науки щодо формування структури права. Інформаційне право є найбільш динамічною галуззю з посеред інших. А тому й виникнення нових підгалузей, інститутів інформаційного права є закономірним та очевидним результатом еволюції цієї галузі права.

Як ми з'ясували вище, правове забезпечення інформаційної безпеки можна визначити як цілісну систему правового регулювання суспільних відносин, що виникають при протидії загрозам національній безпеці України в інформаційній сфері. Тобто, вказаний правовий феномен має власний предмет правового регулювання. Особливості регульованих ним правовідносин впливають насамперед зі специфіки самої інформаційної сфери життя суспільства, зміст якої становить соціальна діяльність зі створення, поширення, трансформації та споживання інформації. При цьому об'єктом відносин, які належать до такої діяльності, має бути інформація та відповідна інфраструктура.

Водночас, забезпечення інформаційної безпеки є одним із різновидів інформаційної діяльності, яка полягає у виконанні певним суб'єктом в межах свого правового статусу функцій із охорони та захисту інформаційних масивів і технологій, засобів і каналів зв'язку. Ця діяльність спрямована на запобігання загрозам безпеці об'єктам національних інтересів у цій сфері, протидію неправомірним зазіханням різноманітних суб'єктів, що можуть завдати шкоди вказаним об'єктам. Цілком зрозуміло, що саме право є головним засобом і найдієвішим інструментарієм зазначеної діяльності.

Отже, відокремленим предметом аналізованого структурного новоутворення правової системи є суспільні відносини, що виникають при протидії загрозам національній безпеці України в інформаційній сфері. При цьому вказана окремішність зумовлена здебільшого особливостями правового забезпечення інформаційної безпеки як різновиду інформаційної діяльності. Про це може також свідчити структура законодавства, пов'язаного з інформаційною сферою, де правове забезпечення інформаційної безпеки як частина інформаційної діяльності представлене такими щільно взаємопов'язаними складовими, як захист державної, комерційної, банківської, лікарської та іншої таємниці, персональних даних, захист від розповсюдження підривної, шкідливої, недостовірної інформації тощо.

Відтак, убачається нагальна потреба чіткого правового врегулювання суспільних відносин у вказаній сфері, виокремлення у вітчизняній правовій системі структури, відповідальної за правове забезпечення інформаційної безпеки. Це створить умови для системного, комплексного розгляду законодавчих положень щодо забезпечення інформаційної безпеки, оперативного виявлення та усунення прогалин і суперечностей в них.

Таким чином, поряд із зазначеним вище виокремленням предмета правового регулювання формується новий комплексний інформаційний феномен – інформаційне право, а в межах останнього й на основі чинного вітчизняного законодавства – модель формування утворення з правового забезпечення інформаційної безпеки.

Відомі дослідники інформаційного права В. Пилипчук та В. Брижко розкривають актуальність проблеми формування нормативно-правової бази у сфері інформаційних відносин та її подальшого розвитку в контексті євроінтеграції України, імплементації норм європейського та міжнародного інформаційного права в інформаційне законодавство України, а також проблеми систематизації національного інформаційного законодавства. При цьому, до основних напрямів упорядкування та регулювання інформаційних відносин, які складають правове поле інформаційної діяльності, відносять й інформаційну безпеку держави [10, с. 11, 18].

Як бачимо, потреба у формуванні такої комплексної правової галузі, як інформаційне право, цілком об’єктивно випливає із самої його природи й зумовлена наведеними вище чинниками. Нагальність і різнобічність питань, пов’язаних з інформацією, кількість котрих з останньої чверті ХХ століття зростає ледь не з геометричною прогресією, зумовлює необхідність виокремлення відповідних суспільних відносин і формування усередині галузі спеціалізованих інститутів, підгалузей та інших структурних утворень, які мають свій специфічний предмет правового регулювання. Цей предмет – багатоманітні різновиди відносин у різних сферах й умовах діяльності, пов’язаних з одним об’єктом – інформацією.

Такими структурними утвореннями галузі інформаційного права є інститути, тобто підпорядковані єдиній меті сукупності нормативно-правових актів і положень, які регулюють усе розмаїття відносин у сфері створення й використання інформаційно-комунікаційних ресурсів і технологій, захисту законних інтересів суб’єктів цієї діяльності тощо. Зрозуміло, що вказані об’єктивні потреби зумовили не лише сплеск наукових досліджень проблематики, скажімо, комерційної таємниці чи захисту персональних даних, а і прийняття останнім часом низки відповідних законодавчих актів.

Цілком очевидним є тісний взаємозв’язок забезпечення інформаційної безпеки з іншими складовими частинами інформаційного права, а також багатьох інститутів інших галузей права. Так, функції забезпечення інформаційної безпеки здійснюються при:

- підтриманні правових режимів певних видів інформації;
- забезпечення відповідальності за порушення нормативних вимог щодо інформаційної безпеки;
- встановленні правового режиму інформаційних ресурсів інформаційних технологій та ін.

Таким чином, ґрунтуючись на загальній теорії систем, нами встановлено, що у вітчизняній системі права з’явився новий елемент, котрий регулює відносини, пов’язані з правовим забезпеченням інформаційної безпеки, а також проаналізували причини й передумови його виникнення. Головними чинниками цього є передусім бурхливий розвиток інформаційних технологій, значне підвищення вагомості інформаційних ресурсів; формування на цьому ґрунті нових суспільних відносин, пов’язаних з інформацією, а також становлення в Україні інформаційного суспільства; виникненням загроз людині, суспільству й державі у цій сфері.

Тому ми підтримуємо думку О. Яреми, що правове забезпечення інформаційної безпеки є частиною системи інформаційного права, що обумовлено комплексною природою інформаційного права [11, с. 251]. Проведений аналіз зазначених передумов дає підстави стверджувати, що вирішальними у виникненні в системі вітчизняного

права нового структурного елемента, пов'язаного із правовим забезпеченням інтересів суб'єктів інформаційних відносин, стали три групи чинників, сталих тенденцій інституційного характеру.

Це, *по-перше*, величезне зростання ролі й значущості інформації в усіх сферах життєдіяльності, масовості використання відповідних засобів і технологій; розвиток на цій основі інформаційного суспільства та інформаційних суспільних відносин. Зрозуміло, вказані процеси мають не лише позитивний бік. Навколо інформаційних ресурсів і технологій виникають конфлікти інтересів суб'єктів інформаційних відносин, загрози їх життєво важливим інтересам. Усі ці питання потребують регулювання, захисту й забезпечення правовими засобами.

По-друге, у процесі діяльності щодо забезпечення інформаційної безпеки як різновиду інформаційних правовідносин виникають відносини, пов'язані із захистом відповідних законних інтересів особи, суспільства й держави від зовнішніх і внутрішніх загроз, і, таким чином, виокремлюється новий предмет правового регулювання.

Нарешті, *по-третє*, це чинники суто науково-методологічні, а також об'єктивний суспільний запит до юридичної науки щодо вдосконалення правового забезпечення інформаційної безпеки.

Усе це зумовило теоретичне обґрунтування існування в системі права такої галузі, як інформаційне право, а також об'єктивне виникнення утворення з правового забезпечення інформаційної безпеки як складової частини останнього – ***підгалузі інформаційного права***.

Утім, слід визнати існування багатьох невирішених проблем. Так, питання інформаційної безпеки в деяких сферах життєдіяльності суспільства залишаються неврегульованими, відповідне законодавство має також певні вади, зумовлені браком структурованості правового забезпечення інформаційної безпеки. Існують у законодавстві недоліки термінологічного плану. Зокрема, відсутнє законодавче визначення поняття “інформаційна безпека держави”, а також низки інших важливих понять, пов'язаних з кібернети́чними загрозами, кібератаками та ін. Отже, вдосконалення чинного законодавства України з питань забезпечення інформаційної безпеки вбачається шляхом закладення міцної теоретичної бази, наукового обґрунтування природи, структури та місця в системі права утворення з правового забезпечення інформаційної безпеки. У цьому контексті слушним є зауваження І. Панової, що сучасна система українського інформаційного права, у зв'язку із розвитком суспільних відносин, зазнає істотних змін, наповнюється новим змістом. З'являються і розвиваються нові правові інститути: захисту персональних даних, інформаційної безпеки, журналістики тощо [12, с. 697].

Що стосується правового забезпечення інформаційної безпеки, то кожен із згаданих інститутів інформаційного права регулює “свою” ділянку цієї сфери. Це, приміром, інститути таємниці, інститут захисту інформації з обмеженим доступом, інститут відповідальності за порушення у цій сфері та ін. Тому, цілком логічним убачається припущення, що правове забезпечення інформаційної безпеки є правовим феноменом, ширшим за традиційне розуміння правового інституту.

Отже, така атрибутивна характеристика природи інформаційного права, як комплексність, стосується й усіх його інститутів. Це, у свою чергу, зумовлює зв'язок між обґрунтуванням комплексної природи сукупності правових інститутів, що регулюють правове забезпечення інформаційної безпеки, та обґрунтуванням її стосунку саме до галузі інформаційного права.

Ще одним системоутворювальним чинником, котрий зумовлює формування галузей права, є предмет правового регулювання. Стосовно правового забезпечення інформаційної безпеки цим предметом ми визначили суспільні відносини, пов'язані із забезпеченням безпеки об'єктів і суб'єктів функціонування інформаційного середовища, що дозволяє віднести це структурне утворення в системі вітчизняного права саме до галузі інформаційного права.

Як уже зазначалося вище, переважна більшість фахівців вважають захист та охорону інформації й відповідних ресурсів, а отже й відносин, що виникають у цій сфері, різновидами саме інформаційної діяльності та інформаційних правовідносин. Продовжуючи логічний ланцюжок від загального – “інформаційна безпека” до окремого – “захист інформації”, доходимо висновку, що забезпечення інформаційної безпеки, як різновид інформаційної діяльності, порівняно із захистом інформації охоплює значно ширше коло питань. Своім об'єктом ця діяльність має інформацію, щодо якої в особи, суспільства й держави виникають певні інтереси, які потребують правового врегулювання – регламентації, правового захисту, забезпечення стану захищеності, охорони тощо. Відносини, які можна назвати інформаційними, що пов'язані з інформацією, відповідними ресурсами, технологіями, комунікаціями, засобами, формують специфічну галузь відносин, котра містить, зокрема, спеціальний комплекс відносин щодо забезпечення інформаційної безпеки держави. У свою чергу, в цьому комплексі виокремлюється певне структурне утворення, пов'язане із правовим забезпеченням інформаційної безпеки. Усе це дає підстави для висновку, що назване нами структурне утворення, яке регулює інформаційні правовідносини, є невід'ємною частиною галузі інформаційного права.

Як уже зазначалося, інформація, середовище та інфраструктура, яке вона створює, сукупність суб'єктів, пов'язаних з ним, суспільні відносини, котрі тут виникають, формують інформаційну сферу життєдіяльності людини, суспільства, держави. Задля забезпечення безпеки цієї сфери держава повинна виробити й утілювати в життя єдину, цілеспрямовану політику. У складних умовах сьогодення українська держава виробила доктрину інформаційної та стратегію кібернетичної безпеки, формується та вдосконалюється відповідне законодавство, спрямоване на захист національних інтересів України у цій сфері.

Нині є всі підстави стверджувати, що в країні створена система, яка досить чітко регулює відносини, що складаються у зв'язку із забезпеченням інформаційної безпеки держави. Деякі аспекти цих відносин внормовані положеннями конституційного, адміністративного та інших “базових” галузей правової системи. Проте, як вище вже доводилося, об'єднати всі ці положення й регулювати цей різновид діяльності має окреме правове утворення зі своєю власною структурою (комплексні інститути, субінститути тощо) та внутрішньою організацією. Так, до комплексних інститутів правового забезпечення інформаційної безпеки держави належать:

- інститут таємниці (державної, комерційної, лікарської та ін.);
- інститут захисту інформації, який містить субінститут ліцензування діяльності у цій сфері, субінститут захисту персональних даних;
- інститут відповідальності за правопорушення в інформаційній сфері.

Досить ґрунтовною науковою працею дослідження інститутів інформаційного права є стаття О. Баранова “Інститути інформаційного права”, у якій автор їх класифікував за процесом створення інформації (інститут права на свободу думки, інститут ЗМІ тощо), відповідно до процесу поширення інформації (інституту телекомунікацій, інститут поштового зв'язку тощо), інститути забезпечення інформаційної безпеки, у рамках якої

вченим виокремлено суспільні відносини, пов’язані із забезпеченням мінімізації збитку від несанкціонованого поширення, використання і знищення інформації (інститут правового режиму інформації, інститут захисту інформації тощо) [13, с. 40, 42, 43]. Указане самостійне комплексне правове утворення, виходячи із мети діяльності й характеру відповідних суспільних відносин, за допомогою сукупності нормативних правових засобів – дозволів, стимулів, заборон, обмежень тощо – має формувати окремий правовий режим. Наприклад, правовий режим захисту інформації з обмеженим доступом передбачає комплексне застосування таких правових засобів, як обмеження, покладання обов’язку, заборона тощо. Прикладом можуть слугувати переліки відомостей, що мають різний ступінь доступу (обмеження), вимога до володільця інформації, що становить комерційну таємницю, вживати певних заходів з її охорони (ставлення в обов’язок), вимога нерозповсюдження персональних даних (заборона).

Формування правової галузі шляхом інтегрування інститутів права вважається багатьма дослідниками найвищим рівнем її побудови. Відомий теоретик права С.С. Алексєєв, зокрема, зазначав, що завдяки виділенню деяких нормативних положень з наступним їх групуванням за певними ознаками в окремих галузях зі споріднених інститутів формуються більші за розміром структури, так звані об’єднання. У кодифікованих нормативно-правових актах такі структури зазвичай утворюють частини чи розділи. Найбільш складним і розвинутим із таких об’єднань визнається правова підгалузь [14].

Оскільки правове забезпечення інформаційної безпеки держави має у своєму складі згадувані вище специфічні правові інститути, але за своєю комплексною природою та предметом регулювання належить до сфери інформаційного права, його не можна вважати самостійною правовою галуззю. Відтак, розглядуваний нами феномен є об’єднанням правових інститутів з високим рівнем диференціації, інтегрування та спеціалізації своїх сукупних структурних елементів, який можна назвати підгалуззю інформаційного права.

Підтвердженням останньої тези може бути й те, що вказане правове об’єднання містить положення, які внаслідок різних видів однорідних відносин (скажімо, пов’язані з державною та іншою таємницею), а також такі, що передбачають набуття певних прав і обов’язків (приміром, співробітників, котрі працюють з персональними даними). Утім, зазначене питання залишається актуальним у науковому сенсі, позаяк до теперішнього часу не стало предметом самостійного комплексного дослідження.

Тим часом, назріло прийняття єдиного, консолідуючого законодавчого акта з питань інформаційної безпеки, зумовлене об’єктивними реаліями формування підгалузі правового забезпечення інформаційної безпеки – Закону України “Про забезпечення інформаційної безпеки держави”.

Отже, правове забезпечення інформаційної безпеки держави є складовою частиною комплексної галузі інформаційного права, котре, у свою чергу, як і всі інші комплексні галузі, належить до певної “базової” галузі права. Комплексна за предметною ознакою галузь інформаційного права є також комплексною і за методами правового регулювання (дозвіл, заборона, примус, покарання тощо). Відтак, підгалузь правового забезпечення інформаційної безпеки також тісно взаємодіє з такими “основними”, на думку багатьох правників, галузями, як конституційне, адміністративне, цивільне, кримінальне право. Ця підгалузь консолідує норми вказаних галузей, що стосуються сфери регульованих нею відносин, сполучає й застосовує притаманні їм методи, способи, засоби та прийоми правового регулювання.

Зокрема, в інститутах таємниці та захисту інформації, відповідальності за порушення в інформаційній сфері сполучаються методи захисту і примусу з дозволом, а також покаранням.

Слід підкреслити, що наявність приватних інтересів, пов'язаних, скажімо, з комерційною таємницею, за імперативного характеру регулювання не свідчить про перетворення приватноправових відносин на публічно-правові. У першу чергу це стосується комерційної таємниці підприємств, які мають особливо важливе та стратегічне значення як для економіки держави, так і для підтримки життєздатності в цілому.

Висновки.

Підбиваючи підсумки аналізу місця правового забезпечення інформаційної безпеки держави в системі інформаційного права, зазначимо, що, по-перше, вказане правове структурне новоутворення у вітчизняній правовій системі має низку ознак підгалузі інформаційного права. Так, норми, які її складають, підпорядковані єдиній меті правового регулювання – забезпеченню інформаційної безпеки людини, суспільства, держави. Крім того, це утворення має відокремлений предмет правового регулювання, правовий режим, характеризується системним застосуванням притаманних галузі методів правового регулювання, значним інтегруванням та спеціалізацією правових інститутів, що його складають (а у складі останніх – субінститутів).

По-друге, правове забезпечення інформаційної безпеки держави є підгалуззю інформаційного права. Це зумовлено їх комплексною природою, а також тим, що правові відносини, які виникають у зв'язку із забезпеченням інформаційної безпеки, охоплюються загальногалузевими правовідносинами. Водночас, вказана підгалузь є цілком самостійним правовим утворенням, до структури якого входять норми як власне інформаційного права, так і норми та положення інших правових галузей, котрі регулюють специфічні суспільні відносини, які виникають з приводу захисту інформації з обмеженим доступом, ліцензуванням діяльності із захисту інформації, а також норми, що визначають відповідальність за правопорушення в інформаційній сфері.

Нарешті, по-третє, структуру правового забезпечення інформаційної безпеки держави як підгалузі інформаційного права складають інститути таємниці, захисту інформації, відповідальності за порушення у цій сфері тощо.

Використана література

1. Окинавская хартия глобального информационного общества. – (Окинава, 22 июля 2000 года). – Режим доступа : http://zakon5.rada.gov.ua/laws/show/998_163
2. Yarger Richard H, George Barber. The U.S. Army War College Methodology for Determining Interests and Levels of Intensity. Carlisle Barracks, U.S. Army War College, 1997. – Режим доступа : <http://www.au.af.mil/au/awc/awcgate/army-usawc/natinte.htm>; <http://www.au.af.mil/au/awc/awcgate/army-usawc/natinte.htm>
3. Мануйлов Є.М., Калиновський Ю.Ю. Аксиологічний вимір інформаційної безпеки української держави // Вісник Національного університету “Юридична академія України імені Ярослава Мудрого”. – № 3 (34) 2017. – С. 13-30
4. Вебер М. Избранное. Образ общества / М. Вебер : [пер. с нем.]. – М. : Юристь, 1994. – 704 с.
5. Ларін С.В. Сутність та зміст поняття “національні цінності” в контексті сучасних дослідницьких підходів // Вісник НАДУ при Президентіві України. – 2016. – № 2. – С. 44-49.
6. Горбулін В.П. Засади національної безпеки України / В.П. Горбулін, А.Б. Качинський. – К. : Інтер-технологія, 2009. – 272 с.
7. Горбулін В. На захист національних інтересів // Політика і час. – 1995. – № 2. – С. 3-8.

8. Ситник Г.П. Державне управління національної безпеки (теорія і практика) / Г.П. Ситник. – К. : Вид-во НАДУ, 2004. – 408 с.
9. Парахонський Б.О. Національні інтереси України (духовно-інтелектуальний аспект) : монографія / Б.О. Парахонський. – К.: НІСД, 1993. – 43 с.
10. Пилипчук В.Г., Брижко В.М. Проблеми становлення і розвитку інформаційного законодавства в контексті євроінтеграції України // Інформація і право. – № 1(1)/2011. – С. 11-19 с.
11. Ярема О.Г., Єсімов С.С. Предмет правового забезпечення інформаційної безпеки в інформаційному праві // Науковий вісник Львівського державного університету внутрішніх справ. – (Серія Право). – 2016. – № 2. – С. 244-252
12. Панова І.В. Тенденції розвитку системи інформаційного права України на сучасному етапі // Форум права. – 2011. – № 2. – С. 694-699. – Режим доступу : <http://www.nbuv.gov.ua/e-journals/FP/2011-2/11pivnce.pdf>
13. Баранов О. Інститути інформаційного права // Правова інформатика. – № 3 (11)/2006. – С. 39-45.
14. Алексеев С.С. Теория права / С.С. Алексеев. – М. : Издательство БЕК, 1995. – 320 с.

~~~~~ \* \* \* ~~~~~