НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

О. О. Тихомиров

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ФУНКЦІЯ СУЧАСНОЇ ДЕРЖАВИ

Монографія

Київ
Центр навчально-наукових та науково-практичних видань
Національної академії СБ України
2014

УДК 34.096+321.01
ББК 67.9(4УКР)301.15
Т 46

Рецензенти:
К. І. Бєляков – доктор юридичних наук,
старший науковий співробітник;
С. Д. Гусарєв – доктор юридичних наук, професор;
А. І. Марущак – доктор юридичних наук, професор

Рекомендовано до друку Вченою радою
Національної академії Служби безпеки України,
протокол № 6 від 3 грудня 2013 року

Тихомиров О. О.

Т 46 Забезпечення інформаційної безпеки як функція сучасної держави : моногр. / О. О. Тихомиров ; заг. ред. Р. А. Калюжний. – Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. – 196 с.

Здійснено теоретико-правове осмислення забезпечення інформаційної безпеки як функції сучасної держави. Сформовано методологічний підхід, який дозволяє розглядати забезпечення інформаційної безпеки як своєрідну діяльність, одним з основних, але не єдиним суб'єктом якої є держава. Структуровано зміст цієї діяльності, охарактеризовано його елементи в контексті становлення інформаційного суспільства й розбудови правової держави. Надано правову інтерпретацію інформаційної безпеки та визначено загальні гарантії її забезпечення в правовій сфері.

Для науковців, викладачів, аспірантів, студентів і курсантів, усіх, хто цікавиться правовими проблемами інформаційної безпеки.

УДК 34.096+321.01
ББК 67.9(4УКР)301.15

ЗМІСТ

ВСТУП

Важливими напрямами розвитку України в сучасних умовах глобалізації світу є інтеграція у світовий та європейський інформаційний простір, розроблення і впровадження в усі сфери суспільного життя інформаційно-комунікаційних технологій, подальший розвиток інформаційної культури особи, забезпечення інформаційної відкритості діяльності органів держави та місцевого самоврядування, становлення інформаційного суспільства загалом.

Стрімкий розвиток інформаційно-комунікаційних технологій на межі XX–XXI століть призвів до виникнення низки нових загроз світовому і національному поступу, що значно підвищує вимоги до забезпечення національної безпеки України й зумовлює нові завдання і функції української держави та її правової системи. З огляду на проголошення України правовою державою, серед них особливого значення в умовах становлення інформаційного суспільства набуває державно-правове забезпечення інформаційної безпеки. Натомість глобальність, висока динаміка, латентність, спонтанність виникнення і зростання загроз в інформаційній сфері суттєво ускладнюють діяльність та певною мірою обмежують можливості держави із забезпечення інформаційної безпеки.

Особливої актуальності державно-правовому забезпеченню інформаційної безпеки в Україні надають процеси трансформації державної, правової, інформаційної сфери, що відбуваються останнім часом, зокрема адміністративна й судова реформи, реформа правоохоронних органів, системи забезпечення національної безпеки тощо.

Такі властивості інформаційної безпеки та системи її забезпечення зумовили активізацію їх наукового осмислення в межах не тільки юридичних, а й інших соціально-гуманітарних і технічних наук, зокрема:

– у теорії держави і права її досліджували В. М. Лопатін, Ю. Є. Максименко, А. А. Письменицький, Т. А. Полякова,

Н. В. Римарьова, А. О. Стрельцов, які розглядали теоретико-правові аспекти забезпечення інформаційної безпеки в контексті взаємозв'язків із відповідними державними й правовими явищами;

– у галузевих і прикладних правових науках на проблемах інформаційної безпеки акцентували свою увагу в межах: адміністративно-правового забезпечення – І. В. Арістова, К. І. Бєляков, Б. А. Кормич, Г. М. Красноступ, О. В. Логінов, Н. Б. Новицька; кримінально-правової охорони – Д. С. Азаров, В. М. Бутузов, Н. А. Розенфельд; інформаційного права – О. А. Баранов, І. Л. Бачило, В. Д. Гавловський, М. В. Гуцалюк, Р. А. Калюжний, А. І. Марущак, В. С. Цимбалюк, М. Я. Швець; криміналістики – А. С. Білоусов, Л. В. Борисова, А. Т. Журба, Д. В. Пашнєв; цивільного права – В. С. Дмитришин, А. С. Колісник, О. В. Кохановська, М. В. Селіванов;

– у спеціальних правових дослідженнях інформаційну безпеку в контексті національної безпеки, міжнародних стандартів її забезпечення осмислювали В. Ю. Артемов, В. Т. Білоус, В. П. Горбулін, О. Г. Данільян, О. П. Дзьобань, Г. В. Іващенко, В. А. Ліпкан, Н. Р. Нижник, Г. В. Новицький, М. І. Панов, В. С. Сідак, Г. П. Ситник;

– у соціально-гуманітарних науках вивчалися такі аспекти забезпечення інформаційної безпеки: філософсько-соціологічні (Я. С. Артамонова, М. Ю. Захаров, О. М. Циденова, В. П. Шемякін); політологічні (О. Ю. Борисов, М. І. Бусленко, В. К. Конах, В. О. Козубський, О. О. Ніколаєв); психологічні (Г. В. Грачов, К. Х. Каландаров, С. Кара-Мурза, С. Є. Некляєв, В. В. Остроухов, І. Н. Панарін, Г. Г. Почепцов, Р. Харріс, О. В. Філатов).

Теоретичні та методологічні засади осмислення забезпечення інформаційної безпеки в контексті функцій держави, гуманізації державної влади, становлення громадянського суспільства, затвердження принципу верховенства права, розвитку правової системи розроблені в працях С. С. Алексєєва, М. І. Байтіна, А. Б. Венгерова, С. Д. Гусарєва, Д. А. Керімова,

М. І. Козюбри, А. М. Колодія, В. В. Копєйчикова, В. В. Ладиченка, Л. А. Луць, Н. М. Оніщенко, П. М. Рабіновича, О. В. Цельєва, М. В. Черноголовкіна.

Проте констатувати цілісність і сформованість галузі знань про інформаційну безпеку зарано. Надзвичайна складність та динамічність явища «інформаційна безпека», загальність і глобальність та, водночас, індивідуальність його проявів стосовно різних суб'єктів (індивідів, організацій, суспільств, держав) і сфер їх життєдіяльності зумовлюють властивості інформаційної безпеки як об'єкта міждисциплінарного наукового пізнання. Це висуває високі вимоги до об'єктивності й обґрунтованості наукових досліджень, системності взаємозв'язків між ними, що має забезпечуватися виваженою методологічною базою із єдиною міждисциплінарною основою і певною інтеграцією методологічних підходів різних галузей науки. Такі дослідження сприятимуть осягненню інформаційної безпеки загалом і окремих її аспектів в умовах науково-технічного прогресу й сучасних суспільних перетворень світового, регіонального та національного масштабу, зокрема правової системи суспільства, держави як соціального інституту, людини як представника інформаційного і громадянського суспільства.

Отже, сучасний стан, значущість і перспективи розвитку інформаційного простору, невиправдані сподівання на ефективність саморегуляції Інтернету та інших глобальних інформаційних мереж доводять необхідність виваженого державного впливу в інформаційній сфері на національному й міжнародному рівнях, особливо стосовно забезпечення інформаційної безпеки. Ця необхідність додатково посилюється новітніми проблемами інформаційної безпеки – захистом інформаційного суверенітету держави, забезпеченням безпеки в кібернетичній сфері, зокрема протидією кіберзлочинності й кібертероризму, захистом критичної кібернетичної інфраструктури держави та іншими.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ФУНКЦІЇ СУЧАСНОЇ ДЕРЖАВИ

1.1. Напрями й методологія правових досліджень інформаційної безпеки

Питання забезпечення інформаційної безпеки сьогодні привертають увагу дослідників різних соціально-гуманітарних та технічних напрямів, що зумовлено міждисциплінарним характером інформаційної безпеки як об'єкта наукового пізнання та залежністю від неї майже всіх сфер сучасного суспільного життя. Ці проблеми породили предметну сферу, певним чином споріднену з достатньо широким спектром соціально-гуманітарних досліджень трансформації явищ соціальної, правової й державної дійсності, які перебувають під значним впливом тенденцій стрімкого інформаційного розвитку, а отже, у прямій залежності від інформаційної безпеки.

У зв'язку з цим спрямованості наукової джерельної бази теоретико-правового осмислення забезпечення інформаційної безпеки як функції сучасної держави характерні дві основні складові:

1) теоретико-правові аспекти розуміння функцій держави та особливостей їх трансформації в сучасних умовах;

2) проблематика інформаційної безпеки в межах теоретико-правових, галузевих і прикладних правових, спеціально-правових та інших соціально-гуманітарних наук.

Перша складова становить сферу наукових досліджень із досить сталими традиціями, яка, поряд із цим, характеризується певним плюралізмом авторських підходів. До другої складової належать наукові розробки, спрямовані на дослідження нових, динамічних суспільних процесів, пов'язаних із безпечним існу-

ванням людини, суспільства й держави в інформаційному просторі, які в умовах стрімкого розвитку інформаційно-комунікаційних технологій отримали надзвичайну актуальність.

Категорія «функції держави» почала активно використовуватись правовою наукою на початку XX століття. На той час вона не була центральним предметом наукових досліджень, проте привертала увагу вчених як важлива характеристика діяльності держави.

Серед перших дослідників, які осмислювали категорію «функції держави», були німецький правознавець Г. Елінек [93] та вітчизняні вчені-юристи В. Ф. Тарановський [306; 307], Г. Ф. Шершеневич [343]. Ними загалом було закладене уявлення про функції держави в тотожності з призначенням традиційних гілок державної влади, що за змістом наближає поняття «функції держави» до понять «форми реалізації функцій держави» і «форми реалізації державної влади», які широко використовуються пострадянською теорією держави як складовою правової науки й політологією.

Активізація вивчення проблем функцій держави в Радянському Союзі спостерігалася в середині 2-ї половини XX століття, що зумовлено, передусім, науковим розробленням концепції соціалістичної держави. У той час поняття «функції держави» набуло чіткого окреслення як характеристика її соціально-класового призначення. При цьому слід зазначити, що багато досліджень мало системно-теоретичний характер, сформувавши теорію функцій соціалістичної держави. Вагомий внесок у розроблення цієї теорії зробили М. І. Байтін [18], А. П. Глєбов [62], А. І. Денисов [82], Л. І. Каск [123], В. М. Корельський [139], В. Л. Тененбаум [310], М. В. Черноголовкін [340] та інші.

Популярність тематики, пов’язаної з функціями держави, та інтенсивність досліджень зумовили певний плюралізм підходів до їх розуміння. Загалом в означений період учені надали багато визначень функцій держави, охопити які можна двома важливими узагальненнями. По-перше, функції держави – це основні або головні напрями, сторони, види її діяльності. По-друге, функції держави відображають її призначення та сут-

ність (класову, соціальну, соціально-класову, загальносоціальну). У цей же період сформувались і традиційні для сучасної теорії держави і права підходи до класифікації функцій держави.

Свій внесок у розробку теорії функцій держави зробили й інші відомі вчені радянського і пострадянського періодів, серед яких А. Б. Венгеров, Ю. Г. Галай, А. Г. Горін, А. І. Корольов, А. П. Косицин, М. Н. Марченко, Л. І. Спірідонов. Функції держави, зокрема з позиції права, розглядалися також у роботах С. С. Алексєєва, Д. М. Бахраха, І. Я. Дюрягіна, В. Б. Ісакова, В. М. Карташова, Д. А. Керимова, В. В. Лазарева, М. І. Матузова, В. С. Нерсесянца, А. С. Піголкіна, С. В. Полеміної, Ю.С. Решетова, І. М. Сенякіна, Ю. О. Тихомирова та інших.

Відчутний поштовх наукове осмислення соціального призначення держави отримало наприкінці 80-х років XX століття. Розпад Радянського Союзу й набуття незалежності його колишніми республіками стали причиною поступового переходу до нової моделі державотворення – правової, соціальної, демократичної держави. При цьому слід зазначити, що теорія функцій соціалістичної держави певною мірою зберегла своє концептуальне значення, а увага дослідників зосередилася на особливостях трансформації конкретних функцій держави в нових умовах.

Попри достатньо високий рівень розробленості проблеми функцій держави, їх дослідження тривають, що доводить актуальність цієї тематики. Проте лише окремі дослідження останнього десятиліття стосувались комплексного з'ясування особливостей функцій держави в нових умовах державотворення. Серед них російські дисертаційні роботи М. О. Бухтерьової «Форми реалізації функцій держави» [44], В. С. Кудрі «Функції правової держави, що перебуває у становленні (на прикладі Російської Федерації)» [152], Г. В. Меліхової «Функції радянської та сучасної російської держави» [181], Л. О. Морозової «Сучасна російська державність (Проблеми теорії та практики)» [188], С. В. Бабаєва «Теорія функцій сучасної російської держави» [17] та українські – О. О. Джураєвої «Функції сучасної держави» [85], Б. П. Ганьби «Системний підхід та його застосування в

дослідженні України як демократичної, соціальної, правової держави» [59], І. І. Мотиля «Становлення та розвиток внутрішніх функцій української держави» [189].

Соціальні функції сучасної держави в межах правової науки досліджували О. В. Бермічева [28], О. С. Мазаєва [172], О. І. Пушкін [263], О. В. Родіонова [271], В. А. Самойленко [281].

Економічні та соціально-економічні аспекти державної діяльності як функції стали предметом економічних і правових досліджень Г. Ю. Атаян [16], О. Г. Варич [45], Г. А. Клочко [127], О. Б. Купцової [155], О. М. Лощихіна [168], О. О. Оськіної [219], С. К. Тимошина [316].

Екологічні функції привернули увагу таких дослідників-юристів, як А. Є. Кадомцева [116], В. С. Миронов [184] та інші.

Цілком логічною в умовах розбудови правової держави є активізація досліджень державної діяльності в напрямі охорони прав і свобод людини та громадянина, забезпечення правопорядку й законності. Цим питанням присвячено дисертації Й. І. Горінецького [67], В. В. Дяконова [92], Р. І. Загідуліна [102], Н. А. Карпової [121], Д. С. Новікова [203], П. В. Онопенка [214], Д. В. Пожарського [235], О. М. Солоненка [287], Д. В. Терьохіна [315] та інших.

У світлі сучасних інтеграційних проблем функції держави розглядали С. О. Кирєєва [126] та В. І. Сало [277].

Особливе значення в умовах становлення інформаційного суспільства та в контексті осмислення державно-правового забезпечення інформаційної безпеки має достатньо новий і мало досліджений напрям – інформаційна функція держави. Йому зокрема присвячено дисертаційні роботи А. М. Васеніної [46] та І. Ю. Нікодімова [200].

До другої складової джерельної бази осмислення забезпечення інформаційної безпеки як функції сучасної держави належать результати наукових досліджень феномену інформаційної безпеки. За глобалізації та становлення інформаційного суспільства інформаційна безпека набуває все більшого значення,

що зумовлює необхідність розгляду її забезпечення на рівні важливої державної діяльності.

Слід зауважити, що важливо розрізняти забезпечення інформаційної безпеки, яка по суті має гуманітарний вимір, та захист інформації, що безпосередньо пов'язаний із технічною діяльністю. Така позиція дозволяє залишити поза межами теоретико-правового обґрунтування своєрідності забезпечення інформаційної безпеки суто технічні та організаційно-правові аспекти технічного захисту інформації.

Правовий характер діяльності сучасної держави зумовлює надзвичайну актуальність і значущість її осмислення з позиції правової науки. Діяльність із забезпечення інформаційної безпеки не є винятком, але, зважаючи на комплексний (міждисциплінарний) характер, вона потребує особливих підходів, які поєднуватимуть методи різних галузей знань, що забезпечить загальну цілісність досліджень інформаційної безпеки.

Правові дослідження сфери інформаційної безпеки нині здійснюються за багатьма напрямами, серед яких теоретико-правові, галузеві й прикладні правові та спеціально-правові дослідження.

Першими спеціальними дослідженнями, в яких почало розвиватися поняття «інформаційна безпека», були дослідження сфери національної безпеки. Саме вони сформували поширений сьогодні підхід, за яким інформаційна безпека розглядається як важлива складова національної безпеки. За такою концепцією її осмислення здійснювали В. Т. Білоус, В. П. Горбулін, О. Г. Данільян, О. П. Дзьобань, Г. В. Іващенко, В. А. Ліпкан, Н. Р. Нижник, Г. В. Новицький, М. І. Панов, В. І. Полевий, В. С. Сідак, Г. П. Ситник та інші [65; 72; 110; 161; 164; 199; 236; 284].

Галузево-правові дослідження інформаційної безпеки активно ведуться за трьома напрямами. Перший і наймасштабніший – це адміністративно-правові дослідження. Їх предметна сфера включає проблеми формування організаційно-правового забезпечення політики інформаційної безпеки в умовах глобалі-

зації, інтеграції, становлення інформаційного суспільства, зокрема захисту персональних даних, інформаційних ресурсів, забезпечення інформатизації, регулювання суспільних відносин щодо комп'ютерних програм, права громадян на інформацію у сфері державного управління, інформаційного забезпечення діяльності різних державних органів, адміністративно-правових форм, засобів і методів забезпечення інформаційної безпеки, а також проблем інформаційної культури в управлінській діяльності та теоретико-методологічних засад інформаційного права [10; 26; 30; 40; 42; 113; 140; 147; 149; 153; 165; 176; 177; 180; 204; 209; 240; 289; 290; 298; 301; 309].

Другий напрям – цивільно-правові дослідження. Основним їх предметом є цивільно-правові аспекти забезпечення інформаційної безпеки, до яких переважно належать проблеми цивільно-правової охорони, захисту та реалізації авторського права в умовах розвитку інформаційно-комунікаційних технологій, авторського права у сфері новітніх комп'ютерних технологій (комп'ютерних програм, комп'ютерних мереж, зокрема Інтернету), а також загальні цивільно-правові проблеми інформаційних відносин [48; 86; 88; 133; 144; 228; 282; 350].

Третій напрям становлять кримінально-правові, кримінологічні й криміналістичні дослідження, актуальність яких зумовлена передусім посиленням такої загрози в інформаційній сфері, як кіберзлочинність, зокрема її проявів – комп'ютерного піратства та шахрайства, хакерства тощо, а також потенційної загрози – кібертероризму. У зв'язку з цим предметом кримінально-правових та кримінологічних досліджень виступають особливості кримінальної відповідальності за злочини у сфері комп'ютерної інформації, шляхи кримінально-правової охорони інформації в комп'ютерних системах та телекомунікаційних мережах, незаконний збут і розповсюдження комп'ютерної інформації з обмеженим доступом, концептуальні питання забезпечення інформаційної безпеки кримінально-правовими засобами та інші [1; 122; 148; 215; 272; 273].

Предметною сферою криміналістичних досліджень є питання методики та особливостей розслідування злочинів у сфері інформаційних комп'ютерних технологій; особливості предмета доказування у справах про комп'ютерні злочини; криміналістичний аналіз об'єктів комп'ютерних злочинів; використання комп'ютерних технологій для фіксації криміналістично значущої інформації у процесі розслідування; використання спеціальних знань при розслідуванні злочинів, учинених із застосуванням комп'ютерних технологій, а також особливості розслідування таких злочинів [31; 32; 38; 99; 190; 221; 229; 237; 280].

Окреме місце в системі правових досліджень інформаційної безпеки займають теоретико-правові дослідження, покликані сформувати цілісну систему правових поглядів на вирішення проблем інформаційної безпеки. До завдань таких досліджень входять правове осмислення інформаційної безпеки як явища загалом та кожної його складової зокрема, визначення шляхів правового впливу на інформаційну безпеку та особливості правових форм її забезпечення, з'ясування взаємозв'язку інформаційної безпеки з іншими правовими явищами, вироблення концептуальних рекомендацій щодо вдосконалення інформаційного законодавства, у тому числі нормативно-правових актів, що визначають фундаментальні основи державної політики забезпечення інформаційної безпеки тощо.

Актуальність теоретико-правових досліджень явищ інформаційної сфери в умовах розвитку інформаційно-комунікаційних технологій і становлення інформаційного суспільства не викликає заперечень, проте слід зазначити, що їх інтенсивність порівняно з іншими напрямами правових досліджень є невисокою. До них належать роботи В. В. Балдицина «Охоронні правовідносини у сфері забезпечення інформаційної безпеки сучасної Росії (Теоретико-правовий аспект)» [19], В. М. Боєра «Інформаційно-правова політика і безпека Росії: теоретико-правовий аспект» [35], Ю. Є. Максименко «Теоретико-правові засади забезпечення інформаційної безпеки України» [174], В. М. Лопатіна «Інформаційна безпека Росії» [167],

О. В. Надигіної «Теоретико-правовий аналіз впливу інформаційних технологій на правосвідомість» [192], Т. А. Полякової «Теоретико-правовий аналіз законодавства у галузі забезпечення інформаційної безпеки Російської Федерації» [239], Н. В. Римарьової «Концептуальні питання формування системи правового регулювання інформаційної безпеки в Російській Федерації» [274], А. О. Стрєльцова «Теоретичні та методологічні основи правового забезпечення інформаційної безпеки Росії» [296], В. М. Супруна «Теоретико-правові основи інформаційного суверенітету» [302], а також О. А. Тамодліна «Державно-правовий механізм забезпечення інформаційної безпеки особистості» [305].

Усеосяжний характер інформаційної безпеки і, відповідно, складність та розгалуженість системи її забезпечення, а також залежність від різноманітних соціально-політичних факторів зумовили необхідність наукового осмислення проблем забезпечення інформаційної безпеки в межах не тільки юридичних, а й інших соціально-гуманітарних наук.

Так, філософсько-соціологічні аспекти інформаційної безпеки досліджували Я. С. Артамонова, Є. О. Архипова, Г. А. Атаманов, М. Ю. Захаров, В. Ю. Триняк, О. М. Циденова, В. П. Шемякін та інші [13; 14; 15; 106; 330; 338]. Тематика їхніх дисертаційних та монографічних робіт орієнтована на соціально-філософський вимір інформаційної безпеки й охоплює її актуальні проблеми в контексті сучасних соціальних перетворень, соціального конфлікту, соціолого-управлінських проблем, безпеки соціуму загалом, а також осмислення як соціокультурного феномену.

Політологічний напрям досліджень інформаційної безпеки розвивали М. О. Богданова, О. Ю. Борисов, М. І. Бусленко, І. І. Залєвська, В. О. Козубський, В. К. Конах, О. О. Левін, О. О. Ніколаєв, І. О. Пеньков, О. А. Судоргін та інші, розглядаючи особливості забезпечення інформаційної безпеки крізь призму політичних і політико-правових проблем життя сучасного суспільства, зокрема удосконалення державної політики

розвитку інформаційного простору та забезпечення інформаційної безпеки в умовах демократичних реформ та інших соціальних трансформацій (глобалізації, інтеграції, інформатизації тощо), а також особливостей забезпечення регіональної інформаційної безпеки та врахування досвіду провідних інформаційно розвинених країн світу [8; 34; 37; 60; 96; 104; 128; 129; 132; 136; 156; 201; 230; 231; 300; 331].

Актуальні нині психологічні аспекти забезпечення інформаційної безпеки в контексті подолання інформаційно-психологічних загроз, до яких насамперед належать інформаційні війни і маніпулювання свідомістю, висвітлені зокрема в роботах Г. В. Грачова, К. Х. Каландарова, С. Кара-Мурзи, С. Е. Некляєва, В. В. Остроухова, І. Н. Панаріна, В. М. Петрика, Г. Г. Почепцова, С. П. Расторгуєва, Р. Харріса, О. В. Філатова [70; 118; 197; 218; 223; 267].

Актуальність, інтенсивність і розгалуженість наукових досліджень інформаційної безпеки, глибинні міждисциплінарні зв’язки між ними і дослідженнями інших явищ висувають високі вимоги до їх методологічної основи. Для таких досліджень оптимальне формування методології може становити окреме наукове завдання, що зумовлено з-поміж іншого тим, що проблеми розвитку інформаційного простору та інформаційно-комунікаційних технологій, їх вплив на державно-правову реальність і навпаки стали нагальними лише наприкінці ХХ – на початку ХХІ століть. Їх дослідження не мають давніх традицій, а різноманітні інформаційні явища та процеси є, з одного боку, своєрідними за своєю природою, а з іншого – універсальними, оскільки взаємопов’язані з різними сферами суспільного буття та його пізнання.

Таким чином, складові методології дослідження державно-правового забезпечення інформаційної безпеки визначаються як загальними та унікальними властивостями предмета дослідження (забезпечення інформаційної безпеки в державному, правовому та соціальному контекстах), так і теоретико-правовою формою його осмислення й відображення за допомогою відповідного понятійно-категоріального апарату, наукової

мови, зумовлених природою та призначенням теорії держави і права в структурі юридичних, соціально-гуманітарних наук, науки в цілому.

Наразі простежуються різні підходи до виокремлення структури методології юридичної науки [3; 98; 117; 130; 131; 143; 169; 266; 269; 308]. Їх аналіз дозволяє констатувати, що методологія сучасних теоретичних правових досліджень не повинна обмежуватися тільки власне науковими методами, а має охоплювати інші форми теоретичного пізнання державно-правової реальності; крім того, сучасній теорії держави і права як юридичній науковій дисципліні притаманна зумовленість світоглядними, філософськими й наукознавчими підвалинами науки XXI століття, новітньою науковою картиною світу права, тенденціями його розвитку тощо [317, с. 248–249].

Трансформація цього твердження стосовно забезпечення інформаційної безпеки як предмета теоретико-правового дослідження дозволяє виокремити декілька основних методологічних складових – загальні засади (світоглядні, філософські, наукознавчі, соціологічні й теоретичні), методологічні підходи, основні наукові методи, предметні теоретичні наукові юридичні знання – і запропонувати таке їх наповнення.

1. Загальні засади:

– сучасний світогляд, що притаманний епосі становлення та розвитку інформаційного суспільства [6; 21; 23; 94; 108; 109; 111; 124; 154; 202; 329; 339; 341; 346; 347], охоплює ідеї інформатизації як провідного фактора майбутнього розвитку людства, який приходить на зміну матеріальному виробництву і, відповідно, матеріальним цінностям, а також ідеї глобалізації, гуманізації та інші, які знайшли своє офіційне визнання в «Декларації тисячоліття» й інших документах ООН, Всесвітнього саміту з інформаційного суспільства тощо [54–58; 77–80];

– онтологічні, гносеологічні, аксіологічні та інші філософські засади, які становлять переважно філософські підходи, розроблені в працях Ю. Хабермаса [328; 351], Г.-Г. Гадамера [29; 91; 327], М. Гайдеггера [97; 103; 135; 158; 159; 330] та інших філософів;

– наукознавчі засади, якими в контексті постнекласичної науки є зокрема інтеграція об'єктивного й суб'єктивного в осмисленні реалій інформаційної безпеки, міждисциплінарність і проблемність її дослідження, спрямованість на вивчення процесів глобалізації, регіоналізації, конвергенції сучасного інформаційного та правового просторів світу [53], а також спеціальна наукова картина світу як єдність і диференціація матеріального та віртуального [109];

– соціологічні засади, що становлять концепції постіндустріального, інформаційного та громадянського суспільства, теорії глобалізації й катастроф, які закладають основні методологічні орієнтири вивчення проблем інформаційної безпеки як складного, багатовимірного та універсального соціального феномену, а також її забезпечення у взаємодії державних і недержавних інституцій, правового та іншого соціального регулювання;

– теоретичні засади державорозуміння, що визначають «параметри» осмислення держави в сучасному світі, зокрема до них належать теорії національної, демократичної, соціальної й правової держави, кожна з яких задає свій «ракурс» вивчення співвідношення держави, права та інформаційної безпеки й особливостей її забезпечення;

– теоретичні засади інтерпретації правових проблем, які зумовлені концепціями нормативізму, позитивізму, природного права, соціологічної та інтегративної юриспруденції, а також комунікативною теорією права [238; 328], яка визначає площину розгляду проблем правового забезпечення інформаційної безпеки.

2. Методологічні підходи

Інтерпретуються як сукупність взаємозалежних і споріднених методів дослідження, що об'єднані домінуючим методом [283; 317]; серед них виокремлюється діяльнісний [74; 87; 275], функціональний [73], системний [59; 275; 336], класифікаційний [183] та інші підходи.

Діяльнісний підхід розроблений у межах «теорії діяльності» і є одним з основних у соціально-гуманітарних науках. До-

цільність і множинність випадків використання діяльнісного підходу в правових дослідженнях інформаційної безпеки зумовлюються його інтерпретаціями в науці як пояснюючого принципу, парадигми, теоретичної моделі та методу наукових досліджень [74; 275], що орієнтують на осмислення державно-правового забезпечення інформаційної безпеки переважно як способу, форми, умови, об'єкта, результату тощо, об'єднаних спільною метою своєрідних діянь певних соціальних суб'єктів.

Діяльнісний метод як домінуючий у цьому підході визначає і відповідну трансформацію інших взаємопов'язаних із ним методів теоретичного дослідження, зокрема: функціонального (напрям та призначення діяльності), структурного (структура діяльності), класифікаційного (види діяльності), інституціонального (норми діяльності), а також методів аналізу, синтезу, порівняння, моделювання тощо.

Фундаментальне значення для дослідження забезпечення інформаційної безпеки саме як функції держави має функціональний підхід, оскільки за наявними в правовій науці традиціями він використовується для дослідження взаємозалежностей державно-правових явищ, їх взаємодії, виокремлення тих чи інших напрямів впливу одного явища на інші [214].

Основу функціонального підходу становлять зокрема такі положення: будь-яке соціальне явище як ціле створюється та існує внаслідок функціональної єдності його складових, їх узгодженого функціонування; функціональність притаманна всім соціальним явищам, відбиває їх призначення, цінність, тому така їх властивість є універсальною; соціальне явище існує, «живе», коли воно функціонує, взаємодіє з іншими явищами, а тому функціональність виступає необхідною властивістю його буття [74, с. 176–177].

У теорії держави і права функціональний підхід найчастіше застосовується для осмислення функцій держави, причому здебільшого під функціями держави розуміють напрями, сторони її діяльності, що розкривають її соціальну сутність і призначення в суспільстві, або ж їх пов'язують із механізмом держави,

формами й методами державної діяльності, діяльністю окремих державних органів, реальністю діяльності держави [206, с. 61], проявами її активності [191, с. 64].

Цей підхід використовується також при дослідженні функцій права як основних напрямів впливу на суспільні відносини з метою їх упорядкування [146, с. 140; 175, с. 109; 285, с. 245] чи реалізації цілей та завдань права, що визначені суспільством [160, с. 150–168; 193, с. 59]; функцій правової системи як напрямів її впливу на суспільні відносини [210, с. 49], процесуальної складової правової системи [49, с. 25–27].

Використання класифікаційного підходу як одного з основоположних дозволяє диференціювати як наукові позиції вчених стосовно проблем соціального призначення держави та інформаційної безпеки, так і реальні державно-правові явища в цій сфері, причому за різними критеріями, як апріорно виокремленими в науковій думці, так і апостеріорними, іманентно притаманними відповідним фрагментам державної й правової реальності (щодо напрямів правових досліджень у сфері інформаційної безпеки; функцій держави; складових інформаційної безпеки; видів об’єктів і суб’єктів, засобів та методів, принципів, правових гарантій, стандартів забезпечення інформаційної безпеки тощо).

Разом із тим, хоча діяльнісний, функціональний та класифікаційний підходи можна уважати необхідними й оптимальними для дослідження забезпечення інформаційної безпеки як функції держави, їх поєднання не є всеосяжним, оскільки не повною мірою відображає результати реалізації державою свого призначення. Тому важливий аналіз функцій держави, зокрема забезпечення інформаційної безпеки, не лише з позиції їх загальної структури або напрямів і змісту державної діяльності, а і як певної цілісності (системи), яка має складну внутрішню структуру і взаємодіє з навколишнім середовищем.

Саме такий ракурс завдає системний підхід. Доцільність і необхідність його використання зумовлені тим, що право, дер-

жава, їх структурні компоненти, а особливо інформаційний простір, є відкритими системами, які знаходяться в стані взаємодії із зовнішнім середовищем, постійно взаємозмінюючись [303, с. 80–81], що дозволяє розглянути забезпечення інформаційної безпеки та її державно-правову складову, з одного боку, як певну систему, а з іншого – як елемент (підсистему) державної й правової систем, системи національної безпеки тощо.

Системний підхід орієнтує на цілісне сприйняття статичних і динамічних, а також структурних компонентів і властивостей інформаційної безпеки та її забезпечення, їх функціональних зв'язків, форм взаємодії з навколишнім соціальним та інформаційним середовищем.

3. Основні наукові методи

Наукові методи як складова методології дослідження забезпечення інформаційної безпеки – це сукупність принципів, правил, прийомів, способів і засобів її пізнання та формування наукових знань щодо неї [170].

Оптимальна реалізація діяльнісного, функціонального, класифікаційного й системного підходів як основи методології дослідження державно-правового забезпечення інформаційної безпеки зумовлює необхідність використання низки наукових методів, які відіграють допоміжну, доповнювальну, забезпечувальну роль:

– загальні методи пізнання – порівняння, аналіз, синтез, абстрагування, узагальнення, моделювання тощо;

– філософські методи – комунікативний, феноменологічний, діалектичний, герменевтичний, аксіологічний, антропологічний;

– загальнонаукові (універсальні) методи – структурний, синергетичний, історичний;

– частково-наукові методи (мають певні обмеження, тому застосовуються окремими групами наук і для дослідження певних предметів та їх властивостей) – статистичні, математичні, конкретно-соціологічні, психологічні тощо;

– спеціальні методи (притаманні лише окремим наукам), використовувані зокрема для дослідження правових аспектів інформаційної безпеки та її забезпечення, – формально-юридичний і порівняльно-правовий.

4. Предметні теоретичні наукові юридичні знання

Предметні теоретичні наукові знання, використані в теоретичних дослідженнях, можуть утворювати окрему складову методології, оскільки в такому разі вони перетворюються на наукові методи, особливості застосування яких визначаються своєрідністю знань, їх призначенням, функціями, понятійним апаратом тощо [196, с. 139–140].

Такі знання як спеціальні методи можуть спрямуватись на осмислення державних і правових аспектів забезпечення інформаційної безпеки, виявлення і дослідження його нових властивостей. До них зокрема належать такі поняття і їх теоретичні конструкції, як «державна діяльність», «функції держави», «механізм держави», «правове регулювання», «інформаційна безпека», «загрози інформаційній безпеці» тощо, які з урахуванням їх відповідної адаптації становлять основу понятійно-категоріального апарату дослідження забезпечення інформаційної безпеки як функції держави.

Отже, забезпечення інформаційної безпеки є комплексним завданням, надзвичайно актуальним для подальшого розвитку людства, причому правова наука відіграє в його вирішенні одну з провідних ролей. При цьому не можна констатувати достатню осмисленість сфери інформаційної безпеки, що спричинено не тільки її об’єктивною складністю та динамічністю, які зумовлюють «прогальність» і несистематизованість наукових знань про неї, а й недостатністю методологічної інтегрованості конкретних наукових досліджень у цілісну систему знань про інформаційну безпеку.

Зокрема недостатньо дослідженими сьогодні залишаються такі напрями:

– трансформація національної безпеки та її складових під впливом сучасних глобалізаційних, інтеграційних, інформаційних процесів;

– системність дослідження безпеки і її складових (вироблення комплексних, міждисциплінарних наукових підходів);

– проблеми державно-правового забезпечення інформаційної безпеки в контексті сучасних соціальних трансформацій, зокрема становлення глобального інформаційного суспільства;

– правові властивості та правові гарантії інформаційної безпеки як явища державно-правової дійсності;

– дотримання прав і свобод людини в процесі забезпечення інформаційної безпеки та належної їх реалізації;

– особливості механізмів правового регулювання забезпечення інформаційної безпеки;

– відповідність стану вітчизняного правового регулювання забезпечення інформаційної безпеки міжнародним правовим стандартам та перспективи його розвитку тощо.

Значна частина цих напрямів лежить у площині теоретико-правових досліджень, які мають фундаментальний по відношенню до інших правових досліджень характер і значний природний потенціал вироблення й гармонійного поєднання відповідних методологічних підходів, а також адекватного використання теоретичних і практичних напрацювань дисциплінарного й міждисциплінарного характеру.

1.2. Функції держави в сучасних умовах

Соціальне призначення – одна з ключових характеристик держави в сучасній політико-правовій думці. Для його теоретичного осмислення найчастіше використовуються традиційні для теорії держави і права взаємопов’язані поняття «завдання», «цілі» та «функції» держави. Питання співвідношення цих понять залишається дискусійним, що викликає потребу їх подальшого дослідження, враховуючи також те, що поширення саме функ-

ціонального підходу визначило пріоритетність використання характеристики «функції держави» та нерозривно пов'язаних із нею «форм і методів реалізації функцій держави».

Загальновідомо, що термін «функція» уведено в науковий обіг німецьким ученим Г. Лейбніцем для означення залежності одних процесів або їх змін від інших (у математиці розуміється як залежність однієї величини від інших) [36, с. 1300]. Однак юридична наука, як і інші суспільні науки, досить часто запозичує терміни з інших галузей знань та надає їм своєрідного значення. Так, у соціології термін «функція» означає роль, яку певний соціальний інститут (або окремий соціальний процес) виконує щодо потреб суспільної системи більш високого рівня організації або інтересів класів, які її утворюють, соціальних груп та індивідів [332, с. 719].

Саме тому поняття «функції держави» недоцільно повністю ототожнювати з первинним поняттям «функції» та розумінням його в інших галузях знань, як і недоцільно повністю виключати зв'язок між ними.

Від початку XX сторіччя, коли набула поширення категорія «функції держави», дослідники неодноразово зверталися до проблеми визначення її змісту. Однак єдиного загальновизнаного підходу немає і дотепер, оскільки поняття «функції держави» є складним, багатогранним та різноплановим, що не дає можливості викласти його у відносно короткому формулюванні, зумовлює плюралізм підходів учених до інтерпретації функцій держави і доцільність їх подальшого осмислення в контексті сучасних перетворень держави і суспільства.

Переважна більшість теоретиків права пов'язує функції держави передусім з основними напрямами її діяльності, що набуло широкої популяризації через навчальну юридичну літературу. При цьому конструкція поняття «функції держави», виражена таким чином, має схожі за змістом авторські інтерпретації її розкриття (доповнення), зокрема, як напрямів діяльності:

– в яких виражається і конкретизується класова та загальнолюдська сутність і соціальне призначення держави (М. І. Байтін) [312, с. 61];

– у яких знаходять своє втілення сутність та соціальна спрямованість, завдання й цілі держави (В. В. Копєйчиков) [313, с. 65];

– які розкривають соціальну сутність і призначення держави в суспільстві, при цьому основні функції, на відміну від неосновних, безпосередньо характеризують її соціальну сутність і призначення (П. М. Рабінович) [264, с. 37];

– що виражають сутність і соціальне призначення, цілі та завдання держави з управління суспільством у притаманних йому формах і властивими йому методами (В. М. Корельский) [311, с. 143];

– із вирішення завдань, що стоять перед державою на різних етапах розвитку, за допомогою спеціальних форм і методів їх реалізації; при цьому розподіл функцій на основні та неосновні є умовним (В. В. Оксамитний) [208, с. 222].

Дещо інша позиція В. С. Нерсесянца, яка ґрунтується на ототожненні держави з живим організмом, а її функцій – із формами життєдіяльності такого організму (формами діяльності, що виражають її сутність) [198, с. 256].

Окремо доцільно виділити інтерпретацію функцій держави, здійснену О. В. Суриловим. «Функції держави – це напрями її діяльності або її діяльність у всій повноті напрямів та аспектів. У головних напрямах виражається сутність держави, у всій повноті цих напрямів – її зміст, тобто загальносоціальна роль» [303, с. 136]. Посилаючись на концепцію відомого дослідника теорії функцій соціалістичної держави Л. І. Каска [63; 123], таким чином він акцентує увагу на обмеженості розуміння функцій держави лише як напрямів її діяльності.

Слід зазначити, що Л. І. Каск ще в період формування теорії функцій соціалістичної держави (70-і роки XX століття) намагався подолати недосконалість пізніше традиційних для політико-правової думки підходів і надати теорії функцій держави більшої реалістичності, що може виявитися корисним на сучасному етапі переосмислення відносин держави і суспільства. Прагнучи збудувати зумовлену об’єктивними факторами мо-

дель функцій держави, він підкреслював взаємозв'язок та відносність понять «функції держави» і «структура держави» й обґрунтовував підхід, за якого функції держави не ототожнюються ні з напрямами, ні зі сторонами державної діяльності й виражаються через зміст цієї діяльності. З диференціацією функцій на основні та неосновні Л. І. Каск також не погоджувався у зв'язку з відсутністю чітких її критеріїв, підкреслюючи, що аналіз функцій держави повинен здійснюватись у контексті етапу її історичного розвитку, який і визначає пріоритетність окремих функцій [123, с. 5–16].

У цьому плані також досить цікава думка А. П. Глєбова, який у науковій дискусії щодо функцій держави був опонентом Л. І. Каска і наголошував на неможливості їх зведення ні до «напряму», «сторони» або «змісту» діяльності держави, ні до соціального призначення держави окремо, оскільки і те, й інше є елементами поняття «функція держави», що характеризують лише одну зі сторін. При цьому він визначив функцію держави як «соціально-класове призначення держави, що реалізується в цілеспрямованому її впливі на суспільні відносини (об'єкти функцій)» [62, с. 34]. «Функція держави припускає єдність таких чотирьох елементів: а) об'єкт (вид суспільних відносин: виробничих, ідеологічних, міжкласових тощо); б) соціальне призначення держави певного історичного типу в регулюванні цієї групи відносин; в) практична діяльність держави (з реалізації свого призначення); г) кінцева мета (на досягнення якої спрямована регулююча діяльність держави в рамках цього виду відносин)» [63, с.102–104].

Отже, проаналізувавши певне коло викладених у науковій та навчальній юридичній літературі визначень функцій держави, можна зробити такі узагальнення:

– більшість учених стверджує, що функціям держави як науковому поняттю відведено роль виражати її сутність та призначення;

– функції держави стосовно цілей і завдань є вторинними або формою їх реалізації;

– немає єдиного підходу до визначення сутності функцій держави (під ними або розуміють лише напрями діяльності держави, або ототожнюють їх із формами, сторонами діяльності держави чи із самою діяльністю);

– підкреслюється, що функції держави об'єктивно зумовлені;

– деякі дослідники підкреслюють класовий характер функцій держави, а також уважають його визначальним і для загальносоціальних функцій;

– окремі науковці ставлять під сумнів доцільність визначення функцій держави як «основних» напрямів діяльності.

Зазначене дозволяє виокремити декілька проблемних питань у традиційних варіантах розуміння функцій держави та запропонувати шляхи їх вирішення.

1. Дуалізм у визначенні функцій держави різними авторами, коли вони розуміються як напрями або як види діяльності, доводить обмеженість кожного з названих розумінь і необхідність використання інтегративного підходу, який дозволить відобразити функції держави у всій повноті аспектів, передусім у теоретичному та практичному (реальному). У межах такого підходу розуміння функцій держави як напрямів і видів діяльності будуть нерозривно пов'язані між собою і виступатимуть різними сторонами одного явища. Визначення функцій держави через сукупність узагальнених видів державної діяльності (апріорна модель призначення держави) відображає теоретичний аспект їх розуміння, у якому функції держави не характеризують якусь конкретну державу, а відображають призначення держави певного типу (соціальної, демократичної тощо). Низка напрямів діяльності, визначених у нормативно-правових актах конкретної держави, в межах яких вона здійснює або прагне здійснювати діяльність (апостеріорна модель призначення держави), відображає вже нормативний і практичний (реальний) аспекти розуміння функцій держави.

2. Визначення функції держави тільки як напряму діяльності не узгоджується з поняттям реалізації функцій. Використання словосполучення «реалізація напряму діяльності» є некорек-

тним із точки зору змістового наповнення цих слів. Аналогічну думку висловлює І. І. Мотиль у своєму дисертаційному дослідженні, підкреслюючи недосконаліть ототожнення функцій держави лише з напрямами її діяльності: «…при погляді на поняття «функція держави» тільки як на напрями її діяльності не маємо можливості говорити про їх здійснення, тому що не можна здійснювати «напрями діяльності», можна здійснювати лише діяльність у межах певних напрямів» [189, с. 13].

3. Визначення функцій держави лише як основних напрямів її діяльності теж є достатньо суперечливим, оскільки не можливо встановити чітку межу між основною й неосновною, більш важливою і менш важливою діяльністю держави. Крім того, класифікуючи функції держави, багато авторів розділяють їх за соціальним призначенням (або за значенням) на основні й неосновні (додаткові), що суперечить самому визначенню функцій держави. Тому доповнення «основні» повинно використовуватися лише в розгляді структурного зрізу функцій держави.

Майже кожну основну в структурному аспекті функцію можна розділити на складові, які називають додатковими (неосновними) функціями [264; 312; 313]. Натомість, кожну додаткову функцію по відношенню до її складових так само необхідно вважати основною. Таким чином, функції держави вибудовуються в ієрархічну структуру, на вершині якої опиняється найбільш загально сформульована функція. Такою функцією в сучасних державах є, зокрема, забезпечення національної безпеки, а додатковими щодо неї – забезпечення територіальної цілісності, конституційного ладу, прав і свобод громадян, науково-технічного потенціалу, високого рівня життя населення, інформаційної безпеки тощо.

4. Сутність та призначення держави не є однопорядковими характеристиками, тому не можуть виражатися через одне й те саме коло функцій і потребують розмежування при визначенні функцій держави. Визначене правовими актами призначення держави має потенційний або декларативний характер, зазвичай закріплюється на конституційному рівні й нерозривно пов’язане

з цілями та завданнями держави. Сутність держави переважно виявляється не в тому, які саме цілі та завдання вона перед собою ставить, оскільки дуже часто вони можуть бути лише декларативними, а в тому, наскільки фактично її діяльність відповідає чи не відповідає об'єктивно зумовленому призначенню, тобто в тому, як вона діє, як реалізує свої можливості, що робить для суспільства в реальному житті. Цей аспект недостатньо відображено в наявних визначеннях функцій держави.

М. В. Черноголовкін, визначаючи функції держави як основні напрями або сторони її діяльності з вирішення історичних завдань, підкреслював, що «функції держави покликані відповідати на питання: що повинна робити держава на певному етапі розвитку, на чому повинні бути зосереджені зусилля її органів та установ» [340, с. 5]. Це означає, що функціями конкретної держави необхідно вважати і можливі (потенційні), й реальні напрями її діяльності із забезпечення потреб та інтересів суспільства. З точки зору теорії держави й права, для держав, що обрали демократичний, соціальний і правовий шляхи розвитку, такий підхід цілком обґрунтований, оскільки основою їх результативної діяльності є демократична природа, соціальна спрямованість та правова регламентація.

Так, діяльності правової держави із здійснення своїх функцій завжди передує нормативно-правове закріплення, що визначає первинно-потенційний характер усіх державних функцій. Держава спочатку декларує наміри здійснювати ту чи іншу діяльність, а далі на правовій основі починає діяти. Однак закріплення функцій держави на конституційному рівні ще не гарантує їх ефективної реалізації. Тому потрібний розподіл функцій держави на потенційні (нормативно визначені), які відображають призначення держави, та реально здійснювані (фактичні), що є необхідною стороною характеристики сутності держави. Власне, і термін «функція» (від лат. functio) у перекладі означає «здійснення, виконання», тобто передбачає діяльність та реальність її результатів. Отже, реально здійснюваною може називатися лише така функція держави, яка має ефективні механізми реалізації та реалізується.

Викладене вище підводить до важливого висновку, що функції держави для того, щоб характеризувати її сутність, повинні відображати саме діяльнісну сторону держави. Потенційні функції, що не реалізуються або діяльність держави щодо яких є неефективною, відбивають лише бажане, можливе, задекларoване призначення держави в суспільстві, якому вона може й не відповідати на конкретному етапі розвитку.

Запропонований розподіл функцій держави на потенційні (нормативно визначені) та реально здійснювані надає можливість використання такої додаткової характеристики сутності держави, як співвідношення реально здійснюваних та можливих функцій, що має відображати загальний стан реалізації функцій держави.

5. Акцентування уваги на класовому характері функцій держави є дещо застарілим і значно зменшує універсальність цього поняття. Вчення про класову боротьбу як основу уявлень про виникнення та функціонування держави формувалось у період існування класового суспільства, а держава забезпечувала інтереси економічно панівного класу. Тенденції розвитку сучасних держав постіндустріального етапу свідчать про поступове зникання значної поляризації суспільства й визначають необхідність зміщення акцентів у розумінні функцій держави убік зумовленості їх потребами всього суспільства та належного закріплення й реалізації прав людини.

Значне ускладнення відносин між державою й суспільством, залежність сучасної держави від суспільства та відповідальність перед ним, що визначається правовим характером діяльності держави, стрімкий розвиток громадянського та інформаційного суспільства зумовлюють перерозподіл функцій держави. Функціональне навантаження на державу зменшується через відчуження значного масиву функцій інститутам громадянського суспільства. Властивими державі залишаються лише її невід'ємні функції, які громадянське суспільство самостійно здійснювати не в змозі, зокрема організація забезпечення суверенітету держави, безпеки суспільства, представництво всього

суспільства на міжнародній арені, надання праву позитивних (писаних) форм тощо. Крім того, функції держави набувають визначально-об'єктивного характеру та залежності від потреб усього суспільства. Таке ускладнення характеру виникнення функцій держави висуває нові вимоги щодо розширення їх наявного поняття й поглиблення підходів до його розкриття та аналізу.

Отже, розширення поняття та необхідність зміни підходу до визначення функцій сучасної держави зумовлені двома основними факторами: прямою залежністю діяльності держави та її функцій від загальносуспільних потреб; демократичним, соціальним і правовим характером діяльності держави.

Перший фактор зумовлює складність процесу утворення функцій держави, на який визначально впливають синергетична природа громадянського суспільства та субсидіарні особливості його взаємодії з державою [9; 12; 120; 335]. Тому в межах широкого підходу існування функцій держави необхідно розглядати на всіх стадіях і рівнях, від виникнення необхідності державної діяльності до її реалізації. Другий фактор визначає нормативний характер закріплення функцій держави, тобто обов'язкову правову регламентацію державної діяльності.

Таким чином, можна виділити три рівні існування функцій сучасної держави:

1) ідеологічний – відбиття функції держави в суспільній свідомості як необхідності державної діяльності в певному напрямі, важливому для розвитку суспільства, зумовленої неможливістю її здійснення інститутами громадянського суспільства;

2) інституціональний (нормативний) – відображення необхідності державної діяльності в сукупності взаємопов'язаних правових настанов, які обов'язково повинні набути закріплення у відповідних правовій системі формах позитивного права;

3) прагматичний (фактичний) – втілення функції держави в її практичній діяльності.

Слід зазначити, що запропоновані рівні, а особливо їх послідовність, в окремих випадках можуть змінюватись. Так, юридичне закріплення функцій, що відповідає другому рівню,

неможливе без практичної діяльності із здійснення такої невід'ємної функції держави, як створення правових актів, а це означає, що в такому випадку прагматичний рівень передує інституціональному.

Усі названі вище рівні існування функцій держави для сучасної держави є обов'язковими. Відсутність зумовленості функцій держави суспільними потребами або їх взаємна суперечливість неминуче викличуть суспільне протистояння, що негативно вплине на реалізацію таких функцій, а в гіршому випадку і багатьох інших, та зрештою призведе до відмови держави від не притаманних їй на цьому етапі розвитку функцій. Відсутність нормативної закріпленості функцій держави або недостатній її рівень, наявність значних колізій та прогалин зведуть до мінімуму ефективність діяльності держави або повністю її унеможливлять. А без третього рівня, що відображає реалії діяльності держави і є визначальним для її сутності, виділення функцій держави як поняття взагалі втрачає сенс.

6. Хоча у співвідношенні завдань, цілей і функцій держави, як уважають фахівці, функціям відведено другорядну роль, саме поняття «функції держави» найчастіше використовується для характеристики призначення та сутності держави, тому воно повинно мати гармонійне змістове наповнення.

Враховуючи означені вище проблеми, можна запропонувати такий підхід до розуміння функцій держави.

Функції держави необхідно розглядати у двох аспектах – теоретичному та практичному (реальному). З теоретичного боку функції держави – це те, що повинна робити держава, щоб відповідати обраній теоретичній моделі або декільком із них. Іншими словами, функції держави у теоретичному розумінні – це сукупність видів необхідної державної діяльності, притаманна певній теоретичній концепції або моделі держави (функції правової держави, функції авторитарної держави, функції соціальної держави тощо). Кожній теоретичній моделі відповідає свій теоретичний комплекс функцій.

У реальному житті кожна держава намагається самостійно визначати те, що вона повинна робити, тобто свої функції, або навіть визначає як мету свою відповідність певній теоретичній моделі на конституційному рівні. Так, ст. 1 Конституції України проголошує її суверенною і незалежною, демократичною, соціальною, правовою державою. Таким чином, тільки визнання державою необхідності здійснення діяльності в певному напрямі робить його напрямом діяльності саме цієї держави. Тому під функціями реальної держави необхідно розуміти не теоретичні (гіпотетичні, нереальні) напрями діяльності, а саме задекларовану (заплановану) діяльність держави, або намір діяльності, який у сучасних державах обов'язково відображається у відповідних правових актах [320].

З етимологічної точки зору слово «намір» означає задум, бажання зробити що-небудь [50, с. 724]. Його використання для визначення функцій держави вирішує одразу дві проблеми: по-перше, надає можливість поєднання в одному визначенні декларативного та реально здійснюваного їх характеру, оскільки наміри державної діяльності, враховуючи систематичний характер здійснення функцій держави, будуть існувати незалежно від своєї реалізації; по-друге, узгоджує на філологічному рівні поняття функцій держави з поняттям реалізації функцій держави. Використання словосполучення «реалізація намірів діяльності» теж є коректним і припустимим. Визнаючи напрям діяльності як свій, держава показує саме намір діяти в цьому напрямі, який надалі може реалізовуватись із різними ступенями ефективності або не реалізовуватись взагалі як з об'єктивних, так і суб'єктивних причин (наприклад, забезпечення високого рівня життя населення, екологічної безпеки тощо). Саме ефективність реалізації своїх намірів виступатиме показником відповідності сутності держави її призначенню.

Таким чином, у реальному аспекті функції держави доцільно інтерпретувати через її наміри, що надасть цьому поняттю більшої універсальності. Отже, функції реальної держави – це важливі для існування й розвитку суспільства і власне держави

види діяльності, що визначені її правовими актами та реалізуються державою з певним рівнем ефективності.

У запропонованому підході взято до уваги лише найбільш суттєві ознаки функцій держави, які потребують розкриття й доповнення. У зв'язку з цим, не заперечуючи методологічної цінності інших наукових підходів, важливо враховувати й такі характеристики:

1) функції держави виникають та розвиваються згідно з історичними умовами й об'єктивними закономірностями існування та розвитку суспільства і держави;

2) функції держави характеризуються стійкістю та динамічністю її намірів протягом певного історичного періоду;

3) лише реальні функції, тобто ті, що фактично реалізуються державою, відображають її сутність, всі інші (доктринально сформульовані) вказують тільки на потенційне призначення держави в суспільстві;

4) в теоретичному аспекті доцільно зважати, що в реальному житті здійснення функцій держави повинно мати систематичний характер;

5) функції держави мають загальний характер, тобто зумовлюють діяльність усього її апарату й кожного його органу, а в окремих випадках і всього суспільства.

Сучасна держава здійснює значний масив функцій, зміст яких є надзвичайно різноплановим, що знову виводить наперед проблему характеристики сутності та призначення держави. Виникає необхідність їх додаткового осмислення в контексті сучасних тенденцій суспільного розвитку. Такий аналіз повинен відобразити багатоаспектність розуміння функцій сучасної держави та забезпечити процеси вивчення і порівняння функцій, цілей і завдань різних держав.

Сьогодні поняття «функції держави» і загалом функціональний підхід становлять першооснову досліджень сутності й призначення держави, типології сучасних держав, побудови концептуальних моделей держав, виходячи із системи пріоритетних напрямів їх розвитку [85, с. 7–9]. За допомогою функці-

онального аналізу можна вирішувати проблеми досліджень сучасної соціальної держави й визначення співвідношення соціальної та правової держави, що активізувалися останнім часом [224, с. 7, 8]. Безперечно, результати таких досліджень залежать від глибини осмислення самого поняття «функції держави», не останню роль у якому відіграє застосування класифікаційного методу.

У науковій та навчальній літературі виділяється низка підстав, що виступають як критерії класифікації функцій держави. До класичних (традиційних) критеріїв слід віднести територіальну спрямованість діяльності держави, соціальне значення, час існування (здійснення) функцій та сферу суспільного (державного) життя.

Згідно з першим критерієм функції держави розподіляються на дві групи:

– внутрішні, що здійснюються в межах території держави і є виразом її внутрішньої політики;

– зовнішні, що здійснюються за територіальними межами держави й виражаються у відносинах з іншими державами та міжнародними організаціями. В цих функціях знаходить своє втілення зовнішня політика держави [313, с. 67].

Класифікація за другим критерієм відображає відносну значущість функцій держави, розділяючи їх на основні й неосновні. Основними традиційно називають такі функції, які розкривають соціальну сутність держави, а неосновними – ті, які їх доповнюють [185, с. 131, 139]. Такий поділ функцій є доволі спірним, оскільки в контексті розуміння функцій держави як основних напрямів діяльності, що розкривають її соціальну сутність і призначення в суспільстві, він створює певну невизначеність їх інтерпретації.

Слід зазначити, що внутрішні й зовнішні функції – це два масиви, що також потребують додаткової типологізації. І якщо з поділом функцій на внутрішні й зовнішні погоджуються практично всі дослідники, то подальша їх диференціація характеризується значним плюралізмом.

Аналіз запропонованих різними авторами класифікацій функцій держави дозволяє виділити два підходи:

1) виокремлення як серед внутрішніх, так і зовнішніх функцій держави, великих груп функцій із подальшим аналізом змісту кожної групи окремо, причому критерієм такого розподілу виступає сфера суспільного життя (економічна, політична, гуманітарна та інші);

2) виділення найширших за обсягом функцій, які поєднують у собі низку споріднених взаємопов'язаних напрямів діяльності держави (у такому випадку ці функції здебільшого називають основними функціями держави).

Прихильником першого підходу до розподілу функцій держави є П. М. Рабинович [264, с. 37]. Другий підхід у роботах дослідників трапляється набагато частіше, однак рівень деталізації функцій, запропонований авторами, різниться і назви одних і тих самих функцій держави часто не збігаються.

Так, В. М. Корельський серед внутрішніх функцій держави виділяє охорону форм власності, охорону правопорядку, охорону природи й навколишнього середовища, економічну та соціальну функції, функцію розвитку науково-технічного прогресу; серед зовнішніх – захист країни від нападу ззовні, ведення загарбницьких війн, взаємовигідну торгівлю, підтримку миру [312, с. 151].

М. І. Байтін та І. М. Сенякін поділяють внутрішні функції держави на економічну, соціальну, екологічну, функцію розвитку культури, науки та освіти, функцію оподаткування й стягування податків, а також функцію охорони прав і свобод громадян, усіх форм власності та підтримання правопорядку; а зовнішні – на функцію оборони країни, забезпечення миру, підтримки світового порядку, функцію інтеграції у світову економіку та функцію співробітництва з іншими країнами щодо вирішення глобальних проблем [211, с. 64–74].

В. С. Нерсесянц серед усього різноманіття функцій держави виділяє правоустановчу, правореалізаторську, правозахисну та зовнішньодержавну, при цьому зазначаючи, що перші три є

внутрішніми й пов'язані зі здійсненням внутрішнього суверенітету держави, а четверта – зовнішньою, що характеризує здійснення зовнішнього суверенітету [198, с. 258].

В. В. Оксамитний до внутрішніх функцій відносить політичну, економічну, соціальну, фіскальну, правозахисну, правоохоронну, ідеологічну й екологічну функції; до зовнішніх – функції захисту державного суверенітету, співробітництва з іншими державами та міжнародними організаціями, а також функцію співробітництва щодо вирішення загальносвітових проблем [208, с. 232–234].

Обидва підходи мають певні недоліки. По-перше, будь-який поділ функцій держави за сферами діяльності або за сферами суспільного життя є відносним, що зумовлено характером, складністю та динамічністю суспільного й державного життя. Це означає, що кожну окремо сформульовану функцію держави не можна розглядати як самостійну і незмінну. Насправді функції сучасної держави – це взаємозалежна, взаємодоповнююча, соціально необхідна її діяльність, що постійно вдосконалюється й адаптується до нових суспільних процесів. По-друге, наведені приклади диференціації функцій держави підтверджують суб'єктивність оцінок і неможливість чіткого розмежування основної й другорядної, більш важливої та менш важливої діяльності держави.

Викладене вище свідчить про відсутність єдиного загальновизнаного вирішення проблеми класифікації функцій держави, а розходження в наукових підходах є результатом пошуку компромісу між спрощеним переліком функцій, якого достатньо для концептуального визначення цілей, завдань і призначення держави в суспільстві, й більш глибоким аналізом з урахуванням усіх аспектів функцій держави, що необхідно для пізнання її сутності. Особливої уваги потребує співвідношення задекларованої та реальної діяльності держави, оскільки саме воно визначає ступінь відповідності держави обраній концепції на сучасному етапі її розвитку.

Одне з найбільш вдалих компромісних рішень проблеми класифікації функцій держави запропоноване колективом укра-

їнських учених, які серед внутрішніх функцій виділяють політичну, економічну, соціальну, екологічну, культурну, правоохоронну, а також функцію оподатковування, фінансового контролю, забезпечення реалізації й захисту прав і свобод людини та громадянина; серед зовнішніх – зовнішньоекономічну, підтримки миру між народами і світового правопорядку, дипломатичну, культурну (гуманітарну), інформаційну [314, с. 105–106].

Утім, цей підхід також не позбавлений певних недоліків. Так, залежно від умов існування сучасної держави серед зовнішніх, так само як і серед внутрішніх, функцій можна виділити екологічну, що полягає в участі держави в міжнародних проектах із збереження й поліпшення екологічної ситуації на планеті; у спільній діяльності держав із попередження й ліквідації наслідків екологічних катастроф. Аналогічним чином доцільно розглядати також інформаційну функцію. Інформатизація сучасного суспільства передбачає проникнення інформаційних технологій практично в усі сфери суспільного життя, що надає провідного значення діяльності держави, пов'язаній із забезпеченням вільного обміну інформацією, інтеграцією у світове інформаційне суспільство, забезпеченням інформаційної безпеки тощо.

Така синкретизація класифікації функцій держави знижує актуальність і значущість їх розподілу на внутрішні й зовнішні, що особливо помітно в умовах інтеграційних і глобалізаційних процесів у світовому співтоваристві, які розмивають грань між внутрішньою та зовнішньою сторонами економічної, політичної, соціальної й екологічної діяльності держави, і підтверджується дослідженнями останніх років [85, с. 11; 152, с. 52; 278, с. 92]. Тобто фундаментальні функції держави поступово втрачають домінуюче значення своєї територіальної спрямованості.

Додатковим офіційним підтвердженням цього є зокрема стратегічна програма розвитку «Україна – 2010», яка не містить окремих напрямів внутрішньої й зовнішньої діяльності держави. Всі національні інтереси розглядаються в контексті розвитку людства, а серед пріоритетних завдань називаються підвищення конкурентоспроможності України в глобальній системі

економіки й прискорення розвитку інформаційної сфери як стратегічної наукомісткої галузі економіки та основи проведення ефективної інноваційної політики [259].

Тісний взаємозв'язок, взаємозалежність і взаємодоповнюваність напрямів державної діяльності орієнтують на осмислення феномену «функції держави» як цілісного явища. У такому контексті класифікація функцій держави відображатиме не їх диференціацію, а багатоаспектність розгляду. При цьому обрані критерії в сукупності створять своєрідну систему відносних координат, у якій можна розглядати існування функцій держави, а кожен із критеріїв задаватиме свою площину розгляду будь-якої функції держави як елемента складним чином структурованого цілого, зокрема в такій інтерпретації.

1. *Часовий зріз.* За часом існування функції розглядаються як постійні й тимчасові. Постійні функції властиві державі в різні періоди її існування, а тимчасові зумовлені певною ситуацією або етапом розвитку. Тимчасові функції виникають і зникають залежно від конкретних завдань, які стоять перед державою в певний історичний період (відвернення військової агресії, запобігання й подолання епідемій, подолання наслідків природних катастроф тощо).

2. *Ціннісний (аксіологічний) зріз.* Цей аспект дозволяє охарактеризувати функції держави відносним значенням, у зв'язку з чим вони можуть розглядатися як пріоритетні або другорядні. Реалізація пріоритетних функцій є визначальною для подальшого існування, розвитку держави і суспільства, тому вона повинна мати консолідуючий характер. Зі зміною умов, що впливають на державний і суспільний розвиток, пріоритети діяльності держави можуть також змінюватися й на перший план виходитимуть раніше другорядні функції (наприклад, пріоритетними функціями свого часу були відбудова народного господарства після Великої Вітчизняної війни, боротьба республік Радянського Союзу за незалежність у період його розпаду, ліквідація наслідків Чорнобильської катастрофи).

3. *Структурно-системний зріз.* Кожна функція держави може розглядатися як елемент цілісної ієрархічної системи функцій, будучи натомість субсистемою функцій. Чим нижче стоїть функція держави в цій ієрархії, тим вищий рівень її конкретизації. У такому контексті функції держави можна розглядати як первинні й похідні (функції та субфункції). Первинна функція об'єднує в собі низку тісно взаємопов'язаних похідних функцій, що виступають її структурними елементами, і щодо них має більш високий рівень узагальненості (в такому розумінні забезпечення національної безпеки буде первинною функцією, а забезпечення територіальної цілісності, економічної й екологічної безпеки, підвищення науково-технологічного потенціалу – похідними). Кожна похідна функція може піддаватися аналогічному аналізу й у своїй субсистемі розглядатися як первинна.

Найбільш всеохоплюючу функцію можна назвати «генеральною функцією держави», яка полягатиме у створенні всіх необхідних умов для оптимального розвитку суспільства [292, с. 47–48].

4. *Зріз по лінії «можливе – наявне».* Цей аспект відображає реальність і ефективність діяльності держави щодо реалізації своїх функцій. За реальністю здійснення функції можна розподілити на реально здійснювані й потенційні (декларативні). Реально здійснювані мають ефективні механізми реалізації, а потенційні – лише декларативне закріплення.

5. *Діяльнісний (змістовий) зріз.* У наукових дослідженнях сформувався нерозривний зв'язок функцій держави і напрямів або сторін державної діяльності, а також, як зазначають окремі автори, цілей, методів, форм і засобів цієї діяльності, що зумовлює доцільність розгляду функцій держави з позиції поняття самої діяльності та елементів її змісту (суб'єкти, об'єкти, мета, предмет, засоби та методи досягнення результатів і результати діяльності). Такий аналіз має глибокий комплексний характер і дозволяє оцінити відповідність діяльності держави цілям і завданням, що стоять перед нею на певному етапі.

6. *Соціальний зріз.* Саме ця площина розгляду є найбільш різноплановою, але, водночас, конкретизованою для кожної держави і такою, що визначає її призначення в суспільстві. Складність та динамічність суспільного життя, науково-технічний прогрес, високі темпи розвитку людства в останні десятиліття висувають особливі вимоги до вивчення трансформації соціального призначення держави в контексті розвитку громадянського й інформаційного суспільства, пріоритету прав і свобод людини та громадянина.

Залежно від сфери суспільного життя можна виділити такі групи функцій, об'єднаних спільними змістовими елементами:

– політичні – формування і здійснення внутрішньої політики держави; створення сприятливих умов для реалізації народовладдя; установлення дипломатичних відносин з іншими державами; оборонна діяльність держави, що полягає в захисті економічними, дипломатичними й військовими засобами її суверенітету й території;

– економічні – вплив на сферу економічних відносин шляхом створення сприятливих умов для розвитку виробництва, підтримка і сприяння розвитку всіх форм власності; установлення та здійснення торгово-економічних відносин з іноземними державами, створення і забезпечення функціонування системи оподатковування та контролю законності прибутків індивідів і організацій, а також використання грошових засобів платників податків;

– власне соціальні – створення найсприятливіших умов для усунення суперечностей між різними соціальними верствами населення, реалізації громадянами права на працю, освіту, достатній життєвий рівень, охорону здоров'я тощо;

– екологічні – охорона й забезпечення раціонального використання природних ресурсів, забезпечення екологічної безпеки суспільства, поліпшення екологічного стану планети, участь у попередженні та ліквідації наслідків екологічних катастроф світового масштабу;

– культурні – забезпечення консолідації нації, формування загальної для всієї країни культури, сприяння розвитку культури всіх народів, які проживають на території держави, та встановленню, розвитку культурних зв'язків з іншими державами; підтримка науки, освіти, мистецтва, фізичної культури й спорту; охорона культурної спадщини;

– правоохоронні – контроль за неухильним дотриманням вимог правових норм, протидія злочинності, забезпечення притягнення до юридичної відповідальності винних у правопорушеннях, забезпечення реалізації й захисту прав і свобод людини та громадянина, підтримка миру на планеті й світового правопорядку, боротьба з міжнародним тероризмом, запобігання виникненню міжнаціональних і міждержавних конфліктів і участь у їх урегулюванні тощо;

– інформаційні – забезпечення вільного обміну інформацією в межах країни, сприяння поглибленню інформатизації суспільства та участь у розвитку світового інформаційного простору з метою забезпечення вільного обміну інформацією між країнами, народами й окремими громадянами, забезпечення інформаційної безпеки людини і суспільства.

Запропонований варіант розгляду класифікації функцій держави не є вичерпним – це лише одна з можливих інтерпретацій. Функції держави – динамічне явище, яке постійно адаптується до мінливих умов її існування і тенденцій розвитку. Цей факт зумовлює вплив на зміст функцій сучасних держав значної кількості різноманітних факторів, здатних змінювати пріоритети й обсяги державної діяльності. Такими факторами можуть виступати зокрема розвиток громадянського й інформаційного суспільства, геополітичне становище, різні етнонаціональні чинники, непередбачувані екологічні зміни, науково-технологічний потенціал. Розстановка пріоритетів у діяльності кожної держави має індивідуальний характер, а змістове наповнення найважливіших функцій залежить від реалій її існування на конкретному етапі.

Отже, у теоретичну конструкцію і будь-яку класифікацію функцій держави апріорі закладено певну умовність, що дозволяє їх використання повною мірою лише як елементів теоретико-методологічної основи наукового або навчального пізнання держави як певного соціального інституту.

Поряд із поняттям «функції держави», з метою поглиблення аналізу державної діяльності, її якісної оцінки, осягнення сутності (змісту) державного впливу на суспільні відносини використовуються й інші характеристики. Ними в теорії держави і права традиційно виступають форми та методи реалізації функцій держави, форми й методи реалізації державної влади, механізм здійснення функцій держави тощо, щодо визначення та місця яких у теоретичних знаннях про державу також немає однозначності. Деякі вчені наголошують на нерозривній єдності цих і аналогічних їм понять у межах категорії «функція держави», з чим варто погодитись [17, с. 12; 51, с. 86]. Реалізувати таке поєднання дозволяє комплексна характеристика державної діяльності з позиції її об'єкта й предмета, мети і завдань, принципів, форм, засобів і методів, результатів тощо, яка є продуктом широкого використання положень теорії діяльності та застосування діяльнісного підходу як домінуючого.

РОЗДІЛ 2

ЗАГАЛЬНОТЕОРЕТИЧНІ АСПЕКТИ ДЕРЖАВНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Теоретична конструкція поняття «інформаційна безпека»

Сучасне життя неможливо уявити без глибокого проникнення інформатизації в усі його сфери. Інформаційна розвиненість поступово стає однією з важливих складових, що визначають «образ» сучасної людини, створюючи необхідну основу її повноцінного існування. З кожним роком інформація набуває все більшого загальносуспільного значення, що надає особливу актуальність гуманітарним дослідженням явищ, нерозривно пов'язаних із нею. Як зазначає академік Російської академії наук, ректор Московського державного університету ім. М. В. Ломоносова В. А. Садовничий, «процеси, що відбуваються зараз в інформаційній сфері, привели до виокремлення нової міждисциплінарної галузі наукового знання. В цій галузі необхідно виділити гуманітарні дослідження проблем забезпечення інформаційної безпеки: визначення закономірностей розвитку інформаційної сфери як системоутворювального фактора життя сучасного суспільства, розроблення та обґрунтування критеріїв і методик оцінювання стану інформаційної безпеки, проблеми правового забезпечення інформаційної безпеки, проблеми інформаційно-психологічної безпеки особи та суспільства тощо» [276, с. 13].

Корінням усіх сучасних інформаційних процесів є сутнісні зміни феномену «інформація», усвідомлення яких створює першооснову досліджень інформаційних явищ. Інформація (лат. *informatio*) – відомості про навколишній світ, процеси, які в ньому відбуваються, про події, ситуації, чиюсь діяльність, що їх сприймають людина і живі організми, машини та інші системи

[304, с. 368]. Саме так сучасний тлумачний словник пояснює слово «інформація», яке є фундаментальним для багатьох термінів, сьогодні вже загальновживаних. Схожим за змістом, але з доповненням можливості збереження на матеріальних носіях або відображення в електронному вигляді, є поняття інформації, закріплене українським законодавством [250]. Зрозуміло, що таке визначення відображає лише формальний бік цього явища і не враховує його соціального значення як цінності, товару, влади, зброї для нападу й захисту, потенціалу для розвитку і причини деградації, світогляду, засобу взаємодії тощо.

Глибина осягнення феномену «інформація» впливає на усвідомлення низки явищ, які визначають майбутнє людства. Для їх позначення сформувався цілий термінологічний комплекс, до якого можна віднести такі терміни, як інформатизація, інформаційна сфера, інформаційне суспільство, інформаційний простір, інформаційний ресурс, інформаційна система, інформаційна інфраструктура, інформаційна безпека, інформаційний суверенітет тощо. Динаміка трансформації інформаційних явищ сьогодні є найвищою, що зумовлює необхідність їх дослідження в нових реаліях суспільного життя.

Останнім часом інформаційна безпека та її окремі аспекти стали предметом численних праць російських та українських дослідників. Однак проблема усвідомлення цього явища залишається відкритою, зважаючи на надвисокі темпи розвитку суспільних відносин в інформаційній сфері. Цей факт пояснюється передусім розширенням можливостей інформаційного впливу на суспільні відносини, що спричиняє виникнення нових загроз суспільній безпеці та зумовлює необхідність оновлення і вдосконалення системи її забезпечення. Крім того, саме поняття інформаційної безпеки потребує постійного переосмислення внаслідок швидких сутнісних змін феномену інформації та домінування тенденцій розвитку світового суспільства, яке все більше отримує «інформаційний» вимір.

Масштабність сучасних перетворень інформаційної сфери є причиною виникнення низки практичних і теоретичних про-

блем, що особливо актуалізують необхідність уточнення поняття інформаційної безпеки та надання йому більш широкого й системного характеру.

По-перше, розвиток методів обміну та поширення інформації, пов'язаний із безпрецедентними темпами науково-технічного прогресу в галузі телекомунікаційних технологій, призвів до виникнення практично необмежених можливостей маніпулювання свідомістю індивідів за допомогою поширення неправдивої або викривленої інформації. Все частіше для розпалювання масштабних соціальних конфліктів інформація використовується як зброя масового ураження, ефективність дії якої залежить від рівня розвитку індивідів та їх обізнаності з політичною ситуацією. Це свідчить про підвищення важливості психологічної складової інформаційної безпеки, яку в наукових дослідженнях прийнято називати інформаційно-психологічною безпекою особи [95, с. 47–51].

В умовах відсутності своєчасної та достовірної інформації людина стає роззброєною перед дезінформаційним впливом, не може адекватно сприймати й осмислювати різноманітні загрози її існуванню та відповідати на них. Разом із розвитком інформаційно-комунікаційних мереж, зокрема швидкісного інтернету, це створює сприятливі умови для діяльності іноземних спецслужб і політичних організацій із поширення дезінформації з метою впливу на суспільну думку та маніпулювання масовою свідомістю, що стає однією з пріоритетних загроз інформаційній безпеці [243]. Тому низька якість інформаційного забезпечення суспільства повинна бути визнана загрозою його інформаційній безпеці на державному рівні, що надалі впливатиме на всі складові суспільної безпеки. Вирішення цієї проблеми ускладнюється тим, що політична боротьба за владу як у державі, так і на міжнародній арені переважно заснована на методах ведення «інформаційних війн», а їх викоренення є проблемою загальносвітового масштабу.

По-друге, інформаційні технології охопили всі сфери сучасного суспільного життя, поставивши існування людини в

повну залежність від нормального функціонування інформаційно-комунікаційних систем. Під впливом цього фактора важко спрогнозувати наслідки зниження рівня інформаційної безпеки в одній окремій галузі діяльності, оскільки це миттєво може поширитися на всі інші галузі. Отже, забезпечення інформаційної безпеки повинно стати одним з пріоритетних завдань соціальної політики.

По-третє, окремою проблемою наукових досліджень є установлення місця інформаційної безпеки в системі загальної суспільної безпеки, а також усвідомлення співвідношення інформаційної безпеки з різними складовими національної безпеки. У межах галузевих досліджень інформаційна безпека традиційно розглядається як невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки [27, с. 175]. Однак необхідно враховувати розширення характеру самої національної безпеки під впливом глобалізаційних та інтеграційних процесів, що, в поєднанні з високими темпами інформаційного розвитку суспільства виводить на перший план проблему переосмислення її інформаційної складової.

Окреслені проблеми зумовлюють перспективу осмислення інформаційної безпеки не як виду національної безпеки, а як відносно самостійного наднаціонального виду всезагальної соціальної безпеки [22, с. 32–35]. У сучасному інформаційному суспільстві вона повинна сприйматися як рушійна сила, сукупність системоутворюючих чинників, підґрунтя для нормального існування соціуму в цілому. Такі властивості інформаційної безпеки висувають особливі вимоги до її наукового дослідження. Обґрунтовано необхідним стає комплексний аналіз інформаційної безпеки та розгляд її на основі низки пов'язаних методологічних напрямів, що засновані на гуманітарній, соціально-інженерній, природно-науковій та математичній парадигмах [75, с. 16–17].

Декларування більшістю держав правового шляху розвитку ставить на особливе місце дослідження правового аспекту забезпечення інформаційної безпеки. Ефективне використання

потенціалу права як загальновизнаного соціального регулятора повинно стати запорукою оптимального функціонування інформаційної системи, гарантування прав і свобод людини в інформаційній сфер, дотримання балансу інтересів усіх суб'єктів інформаційних відносин.

У межах зазначеного підходу необхідно акцентувати увагу на таких позиціях, які сприятимуть осмисленню перспективних змін інформаційної безпеки і дозволять повніше розкрити її зміст.

1. *Підвищення соціальної цінності «інформації».* Інформація, як і все, що надає людству широкі можливості, несе численні нові загрози, усвідомлення й подолання яких є складним процесом. За своєю сутністю інформація – неоднозначне явище. З одного боку, це засіб світосприйняття і взаємодії людей, необхідний для їх розвитку ресурс. З іншого боку, інформація може стати причиною деградації населення, втрати самоідентифікації та національної культури, розпалювання соціальних конфліктів та деструктивного впливу на психіку людини. У цьому контексті значення набуває не тільки наявність або відсутність інформації як сукупності відомостей та знань про навколишній світ, а і її якісний бік, що відображає ступінь придатності для прийняття відповідних рішень. До найважливіших якісних характеристик інформації необхідно віднести повноту, точність, достовірність, своєчасність та законність отримання. У соціальних системах набуття інформацією цих характеристик ускладнюється суб'єктивністю джерел та носіїв інформації, якими часто виступає людина. Тому особливі вимоги висуваються до методик збирання та оброблення статистичної інформації з метою забезпечення її надійності [7, с. 54].

2. *Динамічність перетворень в інформаційній сфері.* Статистичні дані за останнє десятиліття показують незрівнянно високі темпи інформаційно-комунікаційної спроможності суспільства, передусім завдяки швидкісному інтернету, кабельному цифровому телебаченню, мобільному зв'язку, рівень проникнення яких збільшився в десятки разів, зумовивши зокрема і стрімкий розвиток електронних засобів масової інформації.

Україна, як і більшість держав, перебуває на порозі швидкого стрибка у використанні інформаційно-комунікаційних технологій, що призведе до значного ускладнення та урізноманітнення суспільних відносин в інформаційній сфері. Усвідомлення важливості цих відносин підтверджується формуванням та розвитком інформаційного права як самостійного утворення в системі права різних країн і активізацією наукових досліджень у сфері інформаційної безпеки. Інформаційне право як порівняно нова динамічна галузь постійно трансформується, зумовлюючи необхідність систематичного оновлення і вдосконалення своїх позитивних форм.

Визнаючи особливу актуальність діяльності в напрямі інформаційного розвитку суспільства, сучасні держави надають йому пріоритетного значення у своїх програмах перспективного розвитку, а для підвищення ефективності діяльності намагаються об'єднувати свої зусилля. Результатом такої співпраці є Окінавська хартія глобального інформаційного суспільства (Okinava Charter) 2000 р., Лісабонська стратегія (Lisbon Strategy) 2000 р., плани дій щодо розвитку електронної Європи (e-Europe Action Plan), підсумкові документи Всесвітнього саміту з питань інформаційного суспільства (Женева, 2003 р. – Туніс, 2005 р.) тощо.

3. *Взаємозв'язок і взаємозумовленість інформаційного розвитку та розвитку громадянського суспільства.* Сьогодні основні проблеми правового забезпечення інформаційної сфери зумовлені природним відставанням інформаційного права від загальносвітових інформаційних процесів. Інформаційний простір здатний до постійного та стрімкого саморозвитку, тобто йому притаманний синергетичний характер, що орієнтує на осмислення інформаційного розвитку у взаємозв'язку з розвитком громадянського суспільства й навпаки. Інформатизація надає додаткові рівні свободи індивідам та широкі можливості для їх саморозвитку і самоорганізації як членів громадянського суспільства, що є підґрунтям для розвитку інформаційного простору та інформаційної системи суспільства. Ефективність фун-

кціонування цієї системи безпосередньо залежить від її безпеки, забезпечення якої, певною мірою, теж буде характеризуватися синергетичністю і субсидіарністю.

Із цієї позиції функцію забезпечення інформаційної безпеки не можна розглядати як таку, що притаманна лише державі. Вона є функцією кожного суб'єкта інформаційної системи суспільства, і, відповідно, кожен із них виступає суб'єктом забезпечення інформаційної безпеки.

Звичайно, держава займає окреме місце в інформаційній системі. Це єдиний суб'єкт, у потенціалі якого, поряд з економічними, політичними, ідеологічними засобами опосередкованого впливу, закладені можливості прямого управлінського впливу на інформаційні відносини за допомогою правових засобів. Це зокрема зумовлює проблеми концептуального визначення місця держави в системі забезпечення інформаційної безпеки й гарантування балансу інтересів особистості, суспільства, держави в інформаційній сфері.

Управлінську діяльність, що лежить в основі забезпечення високого рівня інформаційної безпеки, доцільно розглядати у двох аспектах: як управління технічними системами та як вплив на соціальні процеси з метою досягнення поставлених цілей. У світлі становлення глобального інформаційного суспільства й визнання його консолідуючою метою людства другий аспект виводить на перший план соціально-гуманітарну парадигму інформаційної безпеки. Отже, для урахування взаємозв'язку інформаційної безпеки з громадянським суспільством виправданим буде осмислення її крізь призму теорії соціальних систем.

Сучасна теорія соціального управління визначає управлінську діяльність як підтримання цілісності будь-якої складної соціальної системи та забезпечення її оптимального функціонування і розвитку [61, с. 12–15]. Саме така достатньо широка інтерпретація поєднує в собі як безпосередню управлінську, так і синергетичну (самоорганізаційну) складові та орієнтує на осмислення інформаційної безпеки зокрема як динамічного стану інформаційної системи, який забезпечує її оптимальний розвиток і функціонування.

Оскільки кожен з елементів інформаційної системи суспільства певним чином здійснює забезпечення її безпеки, то загальний стан інформаційної системи безпосередньо залежить від якостей кожного з її елементів і, відповідно, надійність усієї системи визначається надійністю найслабших її елементів [279]. Держава, маючи найбільші можливості впливу на суспільні відносини, потенційно є найнебезпечнішим елементом, але водночас і основним стимулятором та організатором поліпшення умов життєдіяльності суспільства. Це покладає на державу особливу відповідальність і висуває найвищі вимоги до якості та ефективності її діяльності в інформаційній сфері, зокрема до правового забезпечення інформаційних відносин.

Сприйняття інформаційної безпеки як синергетичного явища розкриває певні діалектичні властивості елементів інформаційної системи: кожен із них одночасно може виступати як об'єктом і суб'єктом забезпечення інформаційної безпеки, так і джерелом потенційних та реальних загроз або каналом їх поширення. Такий погляд дозволяє стверджувати, що можливості забезпечення інформаційної безпеки визначаються можливостями не стільки спеціально призначених для цього державних інституцій, скільки кожного суб'єкта інформаційних відносин щодо власного інформаційного самозахисту. Тому пріоритетним завданням стає підвищення інформаційної культури всіх суб'єктів інформаційних відносин та налагодження їх якісної взаємодії, що створить підґрунтя для забезпечення високого рівня інформаційної безпеки.

Сучасним прикладом оптимізації взаємодії індивідів між собою і з державою на новому рівні є запровадження електронного урядування (e-Government), що має створювати умови для відкритого й прозорого управління суспільними справами на основі широкого використання інформаційно-телекомунікаційних технологій. E-Government – не тільки нова форма державного управління, але й модель глибоких сучасних демократичних перетворень у взаємодії держави, суспільства, громадян, суб'єктів господарювання, основними сферами якої є «електронна демократія», «електронний уряд», «електронна комерція».

Фундаментальною складовою e-Government виступає «електронний уряд» (е-уряд) – єдина інфраструктура міжвідомчої автоматизованої інформаційної взаємодії органів державної влади та місцевого самоврядування між собою, з громадянами й суб'єктами господарювання. До основних його завдань в Україні належать: організація державного управління на основі електронних засобів оброблення, передавання та розповсюдження інформації; надання послуг державних органів усіх гілок влади всім категоріям громадян (пенсіонерам, робітникам, бізнесменам, державним службовцям тощо) із застосуванням електронних засобів; інформування тими ж засобами громадян про роботу державних органів тощо [64].

4. *Залежність від глобалізаційних та інтеграційних процесів.* Початок XXI століття відзначився підписанням 22 липня 2000 року історичного для людства документа – Окінавської хартії глобального інформаційного суспільства. В перших її рядках лідери країн «великої вісімки» визнали розвиток інформаційно-комунікаційних технологій одним з найбільш важливих факторів формування сучасного суспільства, що здійснює революційний вплив на спосіб життя людей, їх освіту й роботу, а також взаємодію уряду та громадськості. Глобальне, відкрите, інформаційне суспільство та єдиний інформаційний простір повинні стати базисом для розвитку передусім глобального фінансово-економічного простору й потенціалом для творчого вирішення економічних, соціальних проблем та реалізації людьми своїх прагнень [207].

Очевидно, що розгортання глобалізаційних процесів не обмежується інформаційною та економічною сферами. Логічним наслідком є подальша глобалізація культурної, правової, наукової, освітньої та інших сфер суспільного життя, яка зумовлює глобальні соціальні проблеми, що можуть набути нищівного для суспільства характеру. Найвідчутніший наслідок інформаційної глобалізації – уніфікація змісту інформації на фоні домінування економічно сильних і політично впливових націй на всесвітньому інформаційному ринку, що кидає виклик куль-

турній самобутності нації [270, с. 193]. Практика європейської інтеграції довела, що втрата самоідентифікації є одним із найнебезпечніших викликів суспільству, який у європейській свідомості поступається місцем тільки тероризму. Причина такої ситуації – циркуляція великих, практично неконтрольованих, потоків інформації, що поступово стирають соціокультурні межі.

Глобалізаційні перетворення зумовлюють необхідність двовекторності інформаційної політики. По-перше, відсутність територіальних кордонів у єдиному інформаційному просторі сприяє набуттю інформаційною безпекою наднаціонального характеру. Загальним завданням світової спільноти стає вироблення єдиних для всіх членів глобального інформаційного суспільства правил поведінки в інформаційній сфері, відображенням яких має бути міжнародне інформаційне право. Міжнародна правова регламентація інформаційних відносин повинна гарантувати досягнення балансу інтересів усіх суб'єктів, недопущення домінування однієї зі світових культур як еталона та сприяння формуванню глобальної інформаційної системи на основі партнерства й консенсусу щодо основних загальнолюдських цінностей [222, с. 17–18].

По-друге, відсутність інформаційних кордонів сприяє розмиванню культур, що може спричинити загальну культурну деградацію людства. Тому особливо важливим є усвідомлення нових інформаційних загроз глобального масштабу та відображення цього у виваженій національній політиці забезпечення інформаційної безпеки суспільства, що орієнтуватиме на виключно конструктивне використання потенціалу інформаційного суспільства. Роль кожної держави в такому випадку полягає у сприянні розвитку інформаційних процесів через створення різноманітних економічних, правових, ідеологічних та інших умов існування національного інформаційного простору.

5. *Місце в геополітичному просторі.* Нові вектори розвитку суспільства створюють нові форми протистояння держав на міжнародній арені. Все частіше військові методи боротьби поступаються місцем сучасним «цивілізованим» методикам ведення ін-

формаційних війн. Сутністю такого інформаційного протиборства є порушення інформаційної безпеки ворожої держави; цілісності системи державного й військового управління; ефективний інформаційний вплив на її керівництво, політичну еліту, систему формування суспільної думки та прийняття рішень, що здійснюється з метою отримання інформаційної переваги у світовому або регіональному просторі [223, с. 173].

Демократизація створює додаткові сприятливі умови для ведення таких війн. «Лише наївна людина здатна вважати, що вибори глави держави або президента в тій чи іншій країні є справою тільки жителів цієї країни і не мають відношення до геополітики» [268, с. 6]. Сучасний процес боротьби за владу характеризується спостереженням із боку не лише сусідніх, а і всіх зацікавлених держав, які за необхідності втручаються, використовуючи передусім економічні та інформаційні важелі впливу.

Україна є унікальним прикладом поля для інформаційних «бойових дій» різних держав. Потенційно вигідне геополітичне становище, на межі східної та західної культур, спрямовує на українське суспільство повсякчас прямо протилежні інформаційні впливи, які створюють ситуацію відсутності стійкості та цілісності державної політики, нелогічності дій державної влади і, зрештою, провокують розвиток політичної атрофії суспільства.

6. *Єдність і взаємодоповнюваність організаційно-правового матеріально-забезпечувального та технічного аспекту забезпечення інформаційної безпеки.* Складна природа інформаційної безпеки та пов’язаних із нею загроз зумовлює доцільність її сприйняття як соціально-технічного феномену, дослідження якого повинно мати міждисциплінарний характер. Технічний захист інформації, відповідні організаційно-правові та матеріально-забезпечувальні заходи необхідно розглядати як складові цілісного процесу забезпечення інформаційної безпеки. Недостатність уваги до кожного з них неминуче призведе до послаблення всієї системи забезпечення інформаційної безпеки [325].

Виходячи з окреслених вище позицій, достатньо сумнівною убачається необхідність пошуку спрощеного підходу до

інформаційної безпеки, оскільки він сприятиме обмеженості розуміння цього феномену. З точки зору раціональності наукового пізнання, доцільне виділення дисциплінарних аспектів розуміння (політичного, правового, соціологічного, ідеологічного, психологічного, технічного тощо) в межах єдиного широкого підходу до інформаційної безпеки як до складного соціально-технічного явища глобального масштабу.

Очевидно, що інформаційна безпека не є явищем найвищого порядку й може розглядатися тільки на основі парадигми соціальної безпеки, із використанням методологічного потенціалу її пізнання, що робить поняття «безпека» базовою категорією для дослідження інформаційної та інших складових безпеки.

Слід зазначити, що наукові підходи «дисциплінарних» фахівців до осмислення інформаційної безпеки ґрунтуються саме на особливостях сприйняття поняття «безпека» різними галузями знань, зокрема:

– психологи розкривають її як відчуття, сприйняття і переживання необхідності в захисті життєво важливих потреб та інтересів людини;

– юристи (правники) – як систему встановлених законом правових гарантій захищеності особи й суспільства, забезпечення їх нормальної життєдіяльності, прав і свобод;

– філософи – як стан, тенденції розвитку й умови життєдіяльності соціуму та його структур, за яких забезпечується збереження їх якісної визначеності та оптимальне співвідношення свободи й необхідності;

– політологи – як властивість (якість) системи і результат діяльності низки систем і органів держави, а також сам процес діяльності, спрямованої на досягнення поставлених завдань щодо забезпечення захищеності особи, суспільства, держави [297, с. 46–47].

Є й інший достатньо поширений етимологічний ракурс визначення безпеки. Тлумачні словники практично однаково трактують її як «стан, коли комусь або чомусь ніщо не загрожує, не викликає занепокоєння» [304, с. 53]. У цьому разі поняття «без-

пека» стає надмірно спрощеним і не відображає реалій існування людського суспільства, яке перебуває в умовах постійних різноманітних загроз, реальних і потенційних, відомих та невідомих, прогнозованих і неочікуваних.

Різноплановість розуміння явища безпеки зумовлює складність і неоднозначність тлумачення інших «безпекових» понять, таких як «національна безпека», «інформаційна безпека», «економічна безпека» тощо. Тому деякі сучасні дослідники сфери національної безпеки підкреслюють необхідність їх розгляду крізь призму теорії соціальних систем, однією з категорій якої є «безпека», що дозволяє на науковому рівні осмислити фундаментальні аспекти розуміння цього явища. Утім, такий підхід зменшує можливості використання напрацьованих ним понять на практиці через їх занадто абстрактний характер.

Зокрема виникає проблема оцінки змін та перетворень, якими охоплено сучасне суспільство, що зумовлює необхідність розроблення системи якісних і кількісних характеристик безпеки, зручних для використання і придатних для стандартизації. Звідси постає проблема гармонізації визначення безпеки як базової категорії в напрямі поєднання в ній як філософського характеру, так і підґрунтя здійснення зручного оцінювання, якому може сприяти використання методів системного аналізу.

Фундаментальною частиною системного підходу до осягнення феномену безпеки має стати його філософсько-соціологічне розуміння, яке на загальнонауковому рівні дозволить уникнути в її дефініціях неоднозначності й суперечливості, пов’язаної із «захищеністю», «інтересами», «потребами», «загрозами», відобразивши при цьому синергетичні властивості безпеки.

Підґрунтя такого розуміння окреслене російським дослідником Г. В. Іващенком. Наголошуючи на недосконалості поширеного визначення безпеки через стан захищеності життєво важливих інтересів особи суспільства і держави від внутрішніх та зовнішніх загроз, він зазначає, що основою усвідомлення безпеки повинен стати діяльнісний підхід, напрацьований соціаль-

ною філософією й теоретичною соціологією. Однак це не означає, що безпеку можна формально розуміти як вид діяльності у відриві від її результатів і умов, у яких вона здійснюється, та можливостей функціонування суб'єкта в цих умовах. Тому безпеку необхідно розглядати як «сукупність умов існування суб'єкта, якими він оволодів (осягнув, засвоїв, створив) у процесі самореалізації і які він, таким чином, здатний контролювати» [110, с. 58].

Тут слід підкреслити, що в синергетичному аспекті простежується певна взаємозалежність умов існування суб'єкта та здатностей або можливостей їх контролю. Умови існування можуть виступати стимулом розвитку здатностей та підвищення спроможності суб'єкта, що надає йому можливості впливати на умови свого існування з метою їх покращання. До таких умов можна віднести і потенційні загрози, рівень яких не тільки не дестабілізує діяльність суб'єктів, а навпаки, спонукає до саморозвитку. Тоді завданням «мінімум» для держави є створення загальних мінімальних умов, що забезпечать саморозвиток і самореалізацію індивідів.

Цей підхід загалом можна узяти за основу з урахуванням згаданих вище напрацювань теорії соціальних систем та управління ними. Квінтесенцією сучасного розуміння безпеки соціальної системи є стабільність її оптимального функціонування й розвитку. Саме за таких умов гарантується достатня захищеність системи. В Україні ідея взаємозв'язку безпеки і стабільного розвитку вже набула закріплення на концептуальному рівні законодавства. Так, Закон України «Про основи національної безпеки України» визначає національну безпеку як «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечується сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам…» [254].

Окреслений вище підхід до поняття «безпека» надає йому абстрактності, притаманної загальнонауковому пізнанню, що створює низку значних переваг. По-перше, поняття безпеки уза-

гальнюється щодо різних суб'єктів (індивідів, організацій, суспільства, держави тощо), що дозволяє його використання як теоретичного компонента методологічної бази системних безпекознавчих досліджень та створення доктринальних актів із виваженим понятійно-термінологічним апаратом. По-друге, такий підхід є універсальним для визначення будь-якого виду або складової безпеки, будь-якого порядку чи рівня – соціальної, національної, політичної, технологічної, воєнної, економічної, інформаційної тощо. По-третє, створюються передумови для вироблення методик зручного оцінювання безпеки, на якому все частіше наголошують сучасні дослідники проблем безпеки, через її стан за допомогою критеріального методу [324].

Проте слід зазначити, що діяльнісний підхід не є всеосяжним, оскільки він суб'єктивізує безпеку. У діяльнісному вимірі вона може розглядатися тільки щодо суб'єкта, адже здійснювати діяльність можуть лише суб'єкти – індивіди або їх колективи (організації). Однак зазначене не є недоліком діяльнісного підходу. Він лише повертає поняттю «безпека» його глибинний соціальний характер, що може зумовити необхідність переосмислення деяких понять та гармонізації термінології загального використання.

В інформаційній сфері прикладом такого поняття є «безпека інформації», яка визначається як захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводять до модифікації, розкриття або зруйнування даних [242]. Проте інформація, набуваючи значення для конкретного суб'єкта (особи, суспільства, держави тощо), стає частиною його «інформаційної складової», яка прямо або опосередковано визначає його сутність. Це означає, що безпека важливої для суб'єкта інформації є, власне кажучи, складовою його безпеки. Шкода цій інформації, і, відповідно, самому суб'єкту може бути завдана через засоби її оброблення. Отже, акцент необхідно робити не на безпеці інформації або безпеці засобів її оброблення, а на надійності функціонування цих засобів. Якщо не обмежуватися суто технічним розумінням надійності як «напрацювання на відмову», то саме надійність та контро-

льованість засобів оброблення інформації є однією з умов безпечного функціонування суб'єктів, у просторі існування яких ці засоби знаходяться.

Підтвердженням наведених суджень є визначення, надане Законом України «Про телекомунікації»: інформаційна безпека телекомунікаційних мереж – здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації [256]. Тобто безпека телекомунікаційної мережі визначається надійністю виконання нею своїх функцій, які полягають у передачі інформації не формально, а з обов'язковим збереженням її якісних характеристик, зокрема повноти, цілісності, своєчасності, конфіденційності.

Щодо поняття «інформаційна безпека», то наразі є численні варіації його трактування. Будучи об'єктом різноманітних галузевих досліджень, інформаційна безпека отримала низку дефініцій як у контексті тематики цих досліджень, так і загальнонаукового характеру. Крім того, не менш важливі нормативні визначення цього поняття, оскільки вони формують загальносоціальне уявлення щодо інформаційної безпеки, виступаючи важливою складовою правового понятійно-термінологічного апарату.

Наведемо деякі з визначень, які наближені до міждисциплінарного характеру інформаційної безпеки.

Нормативні дефініції можуть бути як простими й лаконічними відповідно до вимог законодавчої техніки, так і розгорнутими. Проте і в тому, і в іншому вигляді в них використовуються поняття, які потребують додаткового тлумачення (захищеність, інтереси, потреби тощо).

Так, під інформаційною безпекою Російської Федерації розуміється стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства та держави [89]. Аналогічне визначення повністю підтримує й відомий російський учений В. М. Лопатін [166, с. 79].

За українським законодавством, інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається завдання шкоди через: неповноту, невчасність та недостовірність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [255].

Інформаційна безпека Сполучених Штатів Америки визначається через захищеність інформації та забезпечення цілісності й надійності критичної інформаційної інфраструктури держави в разі випадкових впливів природного чи штучного характеру, навмисних вторгнень або нападів, які можуть спричинити руйнування, переривання, перекручування інформації, що може призвести до широкомасштабних небажаних наслідків політичного, релігійного чи ідеологічного характеру; а також забезпечення формування та подальшого розвитку інформаційних ресурсів з урахуванням інтересів особи, суспільства й держави [137, с. 11].

Більш конкретизоване і наближене до практичної діяльності визначення надане Міжнародною організацією стандартизації (ISO): інформаційна безпека – це захист інформації від широкого спектра загроз із метою забезпечення безперервності бізнесу, мінімізації ризиків бізнесу та максимального збільшення рентабельності й можливостей бізнесу (стандарт ISO/IEC 27002:2005 «Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою») [361].

Серед авторських наукових підходів до осмислення інформаційної безпеки, не применшуючи методологічної цінності всіх інших, можна виділити такі.

Російський дослідник А. О. Стрельцов узагальнено інформаційну безпеку тлумачить як неможливість зашкодження якостям об’єкта безпеки й конкретизує її щодо:

– людини – як неможливість завдання їй шкоди як особистості, соціальна діяльність якої багато в чому базується на усвідомленні отриманої інформації, інформаційній взаємодії з іншими індивідами і предметом якої часто виступає інформація;

– суспільства – як неможливість завдання шкоди його духовній сфері, культурним цінностям, соціальним регуляторам поведінки, інформаційній інфраструктурі та повідомленням, що передаються з її допомогою;

– держави – як неможливість завдання шкоди діяльності держави з виконання функцій управління справами суспільства, предметом якої є інформація та інформаційна інфраструктура суспільства [297, с. 53–58].

Надбаннями української науки є зокрема правові підходи деяких вітчизняних учених. Б. А. Кормич зазначає, що інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування й розвитку людини, всього суспільства та держави [141, с. 142]. Н. Р. Нижник, Г. П. Ситник, В. Т. Білоус інформаційну безпеку розуміють як стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [199, с. 54].

Має рацію і В. М. Панченко, яка наголошує на необхідності поєднання у визначенні інформаційної безпеки гуманітарної та технологічної складових і формулює його таким чином: інформаційна безпека – це такий стан інформаційного розвитку та захищеності особи, суспільства, держави (духовного, правового, технічного), за якого сторонні інформаційні впливи не мають вирішального значення при прийнятті рішень, спрямованих на забезпечення власних (особистих, суспільних, державних) інтересів [225, с. 206].

Вітчизняні фахівці з проблем національної безпеки звертають увагу на необхідність розгляду «інформаційної безпеки» як похідної категорії «національної безпеки» і, відповідно, на-

голошують на спільності методологічного підґрунтя їх осмислення. Зокрема, В. А. Ліпкан, О. В. Логінов, Л. С. Харченко зазначили, що інформаційна безпека – складова національної безпеки, процес управління загрозами та небезпеками, державними й недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [333, с. 47].

Окремої уваги заслуговує підхід Ю. Є. Максименко, яка в процесі теоретико-правового дослідження інформаційної безпеки здійснила детальний аналіз та узагальнення напрямів визначення національної безпеки. Дослідниця використала модель розгляду поняття «національна безпека», запропоновану В. А. Ліпканом, за якою виділяється кілька груп визначень цього поняття: нормативно-правова, доктринальна, енциклопедична [164, с. 415]. На підставі узагальнення різноманіття поглядів учених щодо визначення поняття національної та інформаційної безпеки було виокремлено два підходи:

– «статичний підхід», пов'язаний із визначенням як національної, так і інформаційної безпеки через «стан захищеності (захисту)»;

– «динамічний підхід», згідно з яким під національною та інформаційною безпекою розуміється певний процес, діяльність тощо [174, с. 61].

Зазначаючи обмеженість «статичного підходу» та визнаючи «динамічний підхід» більш адекватним, Ю. Є. Максименко пропонує визначати національну безпеку як «результат управління реальними чи (та) потенційними загрозами (небезпеками)...». При цьому під управлінням розуміється різновид діяльності, що складається зі свідомого цілеспрямованого впливу суб'єктів управління на різні системи з метою підвищення ефективності їх функціонування, приведення у відповідність з об'єктивними закономірностями розвитку [174, с. 36]. А інформаційна безпека інтерпретується як «результат управління реальними чи (та) потенційними загрозами (небезпеками) з метою задоволення національних інтересів людини, суспільства та держави в інформаційній сфері» [174, с. 52].

Не можна не погодитись із прогресивністю і доцільністю осмислення інформаційної безпеки й процесів її забезпечення як управління, про що свідчить також зростання популярності цього підходу серед науковців і виникнення окремого напряму підготовки фахівців із вищою освітою – 170103 «Управління інформаційною безпекою». Утім, необхідно виділити кілька моментів, що мають дискусійний характер.

По-перше, багатогранність явища інформаційної безпеки пояснює його прояв одночасно в кількох змістових компонентах діяльності: інформаційна безпека може виявлятися не лише як результат діяльності, а і як її об'єкт та мета.

По-друге, ототожнення інформаційної безпеки лише з управлінням як окремим видом діяльності дещо обмежує можливості діяльнісного підходу. Очевидно, що й інші види діяльності можуть так чи інакше впливати на інформаційну безпеку і їх результатами, зокрема, може визначатися результат управління.

По-третє, інформаційна, як і будь-яка інша, безпека зумовлюється не лише факторами негативного впливу (загрозами, небезпеками тощо), а й позитивними та нейтральними процесами, які також потребують цілеспрямованого управлінського впливу: позитивні – підтримання та посилення, нейтральні – трансформації в позитивні.

По-четверте, прямий асоціативний зв'язок інформаційної безпеки лише з управлінням приховує синергетичну сторону цього явища, яка є надзвичайно важливою в умовах формування громадянського та інформаційного суспільства.

Таким чином, визначаючи певну змістову спільність згаданих дефініцій, можна констатувати прямий чи опосередкований зв'язок інформаційної безпеки: 1) із належними умовами функціонування або відсутністю умов, у яких може бути завдана шкода; 2) із діяльністю об'єкта безпеки в цих умовах або діяльністю суб'єкта забезпечення безпеки із створення цих умов; 3) із розвитком, який має зумовити інформаційна безпека (це видно з окремих визначень).

Отже, використовуючи потенціал розглянутих вище підходів до визначення інформаційної безпеки та філософсько-соціологічне розуміння безпеки як базової категорії, на загальнонауковому рівні інформаційну безпеку можна інтерпретувати як сукупність умов функціонування суб'єктів в інформаційній сфері та суб'єктивних можливостей їх усвідомлення й контролю. У такому контексті розгляду інформаційна безпека набуває об'єктивно-суб'єктивного характеру.

Відображенням її об'єктивної сторони буде сукупність умов, які концептуально повинні забезпечувати оптимальне функціонування й розвиток суб'єктів, що надає цим умовам відносного та узагальненого характеру. Суб'єктивна сторона інформаційної безпеки знаходить свій вираз у можливостях суб'єктів усвідомлювати та контролювати умови, в яких вони функціонують. Також поняття «інформаційна безпека» набуває гнучкості завдяки відсутності в його змісті певного антагонізму (наявність/відсутність загроз, захищеність/незахищеність, забезпеченість/незабезпеченість розвитку тощо), що дозволяє проводити відносне оцінювання інформаційної безпеки щодо різних факторів (потреб, вимог) за допомогою неполяризованих характеристик, зокрема такої як «рівень інформаційної безпеки».

Запропоноване розуміння, попри його абстрактний характер, не вступає в суперечність із нормативно-правовим розумінням інформаційної безпеки як «стану захищеності...» або «захищеності…», оскільки і те, й інше в сутності є умовами, в яких суб'єкт має функціонувати та розвиватись.

Як правове поняття, зважаючи на вимоги до мови закону та юридичної термінології, інформаційна безпека повинна мати чіткіше окреслену дефініцію, що сприятиме спрощенню процесів усвідомлення цього поняття всіма громадянами. Наявні нормативні конструкції «національні інтереси», «життєво важливі інтереси», «захищеність національних (життєво важливих) інтересів», якими визначається національна безпека та її складові, не є досконалими, проте загалом відповідають необхідному законодавству рівню поєднання повноти, ясності й простоти.

Крім того, вони широко розповсюджені на концептуально-доктринальному рівні українського законодавства і їх зміна наразі нераціональна, оскільки зумовить системні зміни термінології, що призведе до додаткових витрат зусиль та необхідності переосмислення законодавчих підходів широким колом осіб. Поряд із цим, необхідна гармонізація використання таких основних безпекових нормативно-правових категорій, як «національні інтереси», «захищеність», «забезпеченість», що може бути здійснено в процесі поточного удосконалення окремих актів або кодифікації законодавства.

2.2. Структурно-класифікаційна характеристика забезпечення інформаційної безпеки

Сьогодні інформаційна сфера стала інтегруючою основою життєдіяльності суспільства, а забезпечення інформаційної безпеки визнається однією з концептуальних засад його подальшого розвитку. За таких умов особливого значення набуває формування виваженої державної інформаційної політики на основі системних наукових досліджень явищ інформаційної сфери, провідне місце серед яких займає інформаційна безпека.

Одним із важливих етапів системного дослідження інформаційної безпеки є аналіз загальної структури її забезпечення із застосуванням різних методологічних підходів, зокрема системного, функціонального, діяльнісного та класифікаційного. Виокремлення й деталізація складових забезпечення інформаційної безпеки за різними ознаками на основі цих методів сприятиме усвідомленню особливостей кожної з них і, відповідно, формуванню комплексу адекватних заходів державного та недержавного характеру, спрямованих на підтримання оптимального інформаційного розвитку й інтеграції до світового інформаційного простору.

Інформаційна безпека протягом двох останніх десятиліть є об’єктом актуальних наукових досліджень у різних сферах

знань. Висвітлення загальнотеоретичних й окремих аспектів забезпечення інформаційної безпеки на монографічному та дисертаційному рівні здійснило багато вітчизняних і зарубіжних дослідників. Проте особливості загальної структури забезпечення інформаційної безпеки залишаються недостатньо розкритими, що гальмує процеси усвідомлення системності інформаційної безпеки та негативно позначається на формуванні державної інформаційної політики.

Статтею 17 Конституції України забезпечення інформаційної безпеки, поряд із захистом суверенітету і територіальної цілісності, визнається однією з найважливіших функцій держави і справою всього Українського народу. Виходячи з цього, забезпечення інформаційної безпеки доцільно розглядати як цілеспрямовану діяльність, домінуючим, але не єдиним елементом об'єктно-суб'єктного складу якої є держава. Така інтерпретація враховує синергетичні тенденції розвитку сучасного суспільства та субсидіарні особливості його взаємодії з державою й повною мірою відповідає положенням теорії держави і права, згідно з якими функції держави розуміються як напрями, сторони або види державної діяльності.

З метою окреслення особливостей поняття «забезпечення інформаційної безпеки», пов'язаних зі значенням лексеми «забезпечення» і застосуванням діяльнісного підходу, доцільно акцентувати ось на чому.

Тлумачні словники, здебільшого, наводять подвійне семантичне значення слова «забезпечення»:

1) надання, створення засобів та умов, гарантування, захист;

2) засоби або система засобів [50, с. 375].

Названі аспекти, хоча й відповідають його загальноприйнятому тлумаченню, але, з точки зору теорії діяльності, не є рівнозначними. Засоби діяльності обов'язково виявляються у змістових елементах, що становлять незмінну основу самої діяльності [74, с. 89]. Залежно від широти розгляду конкретного виду діяльності засоби можуть як виступати самостійним елементом

її змісту, так і знаходити свій вираз в інших елементах – меті, завданнях та результатах діяльності. Зокрема, організаційну діяльність держави узагальнено можна представити у двох стадіях: перша – створення необхідних засобів та надання їх відповідним суб'єктам, друга – використання засобів суб'єктами у своїй діяльності для вирішення поставлених завдань. У цьому аспекті засоби як такі є завданнями й результатом діяльності, спрямованої на досягнення мети вищого порядку, і перебувають у змістовій єдності із самою діяльністю.

Подібної позиції у своїх дослідженнях дотримується А. О. Стрельцов. Щодо поняття «забезпечення» він підкреслює: «Забезпечення є сукупністю діяльності із забезпечення, засобів забезпечення та суб'єктів забезпечення. Діяльність із забезпечення полягає в наданні допомоги суб'єктам у досягненні поставлених цілей. Засоби забезпечення утворюють сукупність матеріальних, духовних, фінансових, правових, організаційних і технічних засобів, необхідних для діяльності із забезпечення. Суб'єктами забезпечення є індивіди, організації та органи держави, що здійснюють діяльність із забезпечення» [297, с. 44].

Отже, діяльнісний підхід, не створюючи термінологічної дисгармонії, нерозривно поєднує обидва аспекти «забезпечення», під чим слід розуміти відповідну діяльність у всій повноті змістових та структурних елементів.

Системність інформаційної безпеки дозволяє визначити її забезпечення як складний, комплексний вид діяльності, що зумовлює її надзвичайну структурну розгалуженість. Сьогодні загальноприйнятого механізму структуризації забезпечення інформаційної безпеки немає. Для виокремлення складових його загальної структури найчастіше використовуються такі термінологічні конструкції, як «напрями», «механізми» та «шляхи» забезпечення. Однак саме розуміння забезпечення інформаційної безпеки як комплексного виду діяльності дозволяє гармонізувати термінологію і здійснювати не лише структурний, а й глибокий змістовий аналіз, повною мірою застосовуючи потенціал діяльнісного підходу.

Результати аналізу різноманітних джерел свідчать про недостатню розробленість та систематизованість структурних складових забезпечення інформаційної безпеки. На рівні законодавства практично безальтернативним залишається підхід, у межах якого залежно від пріоритетних загроз визначаються напрями забезпечення інформаційної безпеки, об'єднані за традиційними сферами життєдіяльності. Доктрина інформаційної безпеки України, Доктрина інформаційної безпеки Російської Федерації, а також фундаментальні нормативно-правові акти у сфері забезпечення національної безпеки використовують саме такий підхід.

У науковій сфері пріоритет надається класифікації загроз як чинників, що зумовлюють основні напрями або шляхи забезпечення інформаційної безпеки. Водночас не менше пізнавальне значення має класифікаційна характеристика самого забезпечення інформаційної безпеки, здійснена на підставі не лише предмета діяльності (загрози), а й інших критеріїв, що дозволить отримати більш повне уявлення щодо його особливостей.

Осмислення забезпечення інформаційної безпеки як функції держави логічно інтегрує окремі компоненти методології дослідження цих явищ. Тому класифікацію забезпечення інформаційної безпеки доцільно здійснити на основі моделі, використаної для класифікації функцій держави в цій роботі. Кожен обраний критерій такої класифікації розглядається не як підстава диференціації, а як ознака, що задає площину розгляду забезпечення інформаційної безпеки. Застосування цього прийому дозволяє створити теоретичну модель забезпечення інформаційної безпеки, не порушуючи системних взаємозв'язків його складових.

Емпіричною базою класифікації забезпечення інформаційної безпеки саме як функції сучасної правової держави, тобто офіційно визнаної діяльності (регламентованої правовими актами), можуть слугувати положення актів законодавства України, що згідно із Законом України «Про основи національної безпеки України» (ст. 2) становлять правову основу забезпечення ін-

формаційної безпеки, а також актів законодавства інших країн, зокрема Російської Федерації, де простежуються близькі до вітчизняних погляди на проблеми забезпечення інформаційної безпеки.

Серед таких актів, зокрема, закони України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про Концепцію Національної програми інформатизації», «Про Національну програму інформатизації», «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації»; проекти законів України «Про Концепцію національної інформаційної політики», «Про Концепцію державної інформаційної політики»; укази Президента України «Про Доктрину інформаційної безпеки України», «Про Стратегію національної безпеки України»; закони Російської Федерації «Про інформацію, інформаційні технології та про захист інформації», «Про персональні дані», «Про безпеку»; затверджені Президентом Російської Федерації «Концепція національної безпеки», «Концепція державної інформаційної політики», «Доктрина інформаційної безпеки Російської Федерації», «Стратегія розвитку інформаційного суспільства в Російській Федерації».

Зважаючи на окреслені вище методологічні особливості, класифікувати забезпечення інформаційної безпеки можна так.

1. За сферами суспільного (державного) життя:

– забезпечення інформаційної безпеки в економічній сфері;

– забезпечення інформаційної безпеки в політичній сфері;

– забезпечення інформаційної безпеки у воєнній сфері;

– забезпечення інформаційної безпеки в науково-технологічній сфері;

– забезпечення інформаційної безпеки в екологічній сфері;

– забезпечення інформаційної безпеки в соціальній сфері тощо.

Підтвердженням важливості такого розподілу є зосередження на ньому уваги в численних наукових дослідженнях і багатьох нормативно-правових актах доктринального-концептуального рі-

вня, які стосуються інформаційної та національної безпеки. Зокрема українським законодавством інформаційна безпека визначається як невід'ємна складова кожної зі сфер національної безпеки, що закріплено Законом України «Про Концепцію Національної програми інформатизації» та Доктриною інформаційної безпеки України [247; 252].

2. За об'єктами національної безпеки:

– забезпечення інформаційної безпеки особи;

– забезпечення інформаційної безпеки суспільства;

– забезпечення інформаційної безпеки держави [247; 254].

У контексті сприйняття інформаційної безпеки як невід'ємної складової кожної зі сфер національної безпеки проглядається виключна єдність загальних об'єктів національної та інформаційної безпеки. Так, Законом України «Про основи національної безпеки» об'єктами національної безпеки визначено людину й громадянина, суспільство, державу. Доктрина інформаційної безпеки України деталізує особливості цих об'єктів щодо забезпечення інформаційної безпеки, використовуючи поняття життєво важливих інтересів в інформаційній сфері, а саме:

1) особи – забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; недопущення несанкціонованого втручання в зміст, процеси оброблення, передачі та використання персональних даних; захищеність від негативного інформаційно-психологічного впливу;

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

3) держави – недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії інших держав та міжнародних структур; ефективна взаємодія органів державної влади та інститутів громадянського суспільства при

формуванні, реалізації й коригуванні державної політики в інформаційній сфері; побудова та розвиток інформаційного суспільства; забезпечення економічного й науково-технологічного розвитку України; формування позитивного іміджу України; інтеграція України у світовий інформаційний простір [247].

3. За сучасними аспектами розуміння інформаційної безпеки:

– забезпечення інформаційно-психологічної безпеки;

– забезпечення інформаційної безпеки у сфері прав і свобод людини;

– забезпечення інформаційно-технічної (технологічної) безпеки.

Незважаючи на умовність, цей контекст розгляду набуває дедалі більшої популярності в роботах українських та російських дослідників, причому особливу увагу останнім часом привертає виокремлення інформаційної безпеки у сфері прав і свобод людини, а також кібернетичної безпеки, яку певною мірою можна вважати складовою інформаційно-технічної (технологічної) безпеки.

Забезпечення інформаційно-психологічної безпеки полягає в мінімізації негативних впливів на свідомість людини (як громадян, так і державних посадових осіб) та суспільства, пов'язаних передусім із маніпулюванням свідомістю з різною метою, зокрема терористичною, і поширенням суспільно небезпечної ідеології (культу насильства та жорстокості, расизму, радикального націоналізму, порнографії тощо).

Основним змістом забезпечення інформаційної безпеки у сфері прав і свобод людини є недопущення розголошення інформації з обмеженим доступом, порушень права власності на інформацію, неправомірного обмеження свободи слова та доступу громадян до публічної інформації й інших прав і свобод, які належать до інформаційної сфери або реалізуються в ній.

До забезпечення інформаційно-технічної (технологічної) безпеки належить створення можливостей для безпечного формування й розвитку інформаційних ресурсів та інформаційної

інфраструктури, своєчасного виявлення загроз безпеці держави, суспільства, особи в інформаційній сфері та організація ефективної протидії їм за допомогою технічних засобів.

4. *За основними видами інформаційної діяльності:*

– забезпечення законних можливостей створення, збирання, одержання та використання інформації;

– забезпечення законного порядку поширення інформації;

– забезпечення належного зберігання інформації;

– охорона та захист інформації;

– створення і розвиток інформаційних ресурсів.

Основні види інформаційної діяльності були безпосередньо визначені та розкриті попередніми редакціями Закону України «Про інформацію», а державна діяльність, що відповідає цим видам, згідно зі ст. 3 чинної редакції цього закону становить основу державної інформаційної політики України [250]. Відносини у сфері охорони та захисту інформації, забезпечення належного режиму доступу до інформації, що охороняється законом (державної таємниці, конфіденційної, службової інформації тощо), в Україні вже тривалий час є предметом правового регулювання. При цьому питання використання й отримання відкритої соціально необхідної інформації до недавнього часу залишалися поза увагою законодавця.

Ситуація почала поступово змінюватись із затвердженням у 2009 році Доктрини інформаційної безпеки України, якою серед основних засад визначено: свободу збирання, зберігання, використання та поширення інформації; достовірність, повноту й неупередженість інформації; обмеження доступу до інформації виключно на підставі закону. Крім того, з метою створення механізмів реалізації права кожного на доступ до публічної інформації у 2011 році прийнято Закон України «Про доступ до публічної інформації» і внесено зміни до Закону України «Про інформацію» та деяких інших нормативно-правових актів.

5. *За формами державного забезпечення інформаційної безпеки:*

– забезпечення якісного інформування;

– забезпечення процесів інформатизації;
– правова регламентація сфери інформаційних відносин;
– боротьба з правопорушеннями в інформаційній сфері.

Зміст державного забезпечення інформаційної безпеки може інтерпретуватися як система державних гарантій в інформаційній сфері, прямо чи опосередковано визначених фундаментальними нормативно-правовими актами, що регламентують інформаційну сферу суспільних відносин.

Інформування, тобто надання суб'єктам необхідної для функціонування й життєдіяльності якісної інформації, є однією із засад розвитку інформаційного і громадянського суспільства. Оскільки інформація виступає засобом осягнення простору існування суб'єктів, то належний рівень їх поінформованості про процеси, що відбуваються в державі та світі, є необхідним підґрунтям для прийняття адекватних рішень. Особливо гостро проблеми інформування виявляються в напрямах: якісного інформаційного забезпечення діяльності державних органів і посадових осіб; ефективного поширення правової інформації як організаційної основи у важливих сферах суспільних відносин, зокрема у сфері забезпечення інформаційної безпеки; надання своєчасної, повної, неупередженої інформації суспільству щодо діяльності державних органів; об'єктивного та оперативного висвітлення подій як державного, так і світового масштабу.

Так, Доктриною інформаційної безпеки Російської Федерації недоліки інформування відображаються у двох формах: 1) як джерела загроз – недостатня активність державно-владних структур з інформування суспільства щодо своєї діяльності, з роз'яснення ухвалених рішень, із формування відкритих державних ресурсів та розвитку доступу громадян до них; 2) як загрози – низька ефективність інформаційного забезпечення державної політики та блокування діяльності засобів масової інформації [89].

Інформатизація як цілеспрямована діяльність держави полягає в створенні політичних, економічних, технічних та інших умов для інформаційного розвитку суб'єктів, розвитку державного інформаційного ресурсу та оптимізації обміну інформацією шляхом широкого використання інформаційних технологій.

До пріоритетних загальнодержавних проектів інформатизації в Україні згідно з Концепцією Національної програми інформатизації належать: створення національної інформаційно-телекомунікаційної системи; розвиток системи національних інформаційних ресурсів; інформатизація стратегічних напрямів розвитку економіки держави, її безпеки та оборони, соціальної сфери [252]. Відповідно, відставання від провідних країн світу за рівнем інформатизації органів державної влади та місцевого самоврядування, кредитно-фінансової сфери, промисловості, сільського господарства, освіти, охорони здоров'я, сфери послуг і побуту тощо є джерелом загроз інформаційній безпеці.

Правова регламентація сфери інформаційних відносин і боротьба з правопорушеннями в ній є взаємодоповнюючими складовими процесу необхідного унормування «інформаційної» поведінки суб'єктів. Їх правові проблеми мають спільне коріння і зумовлюють розвиток інформаційних правовідносин. Розглядаючи ці питання в контексті розбудови України як правової держави та становлення її правової системи, доцільно звернути увагу на потенційні можливості кодифікації інформаційного законодавства України, яка може забезпечити одночасне вирішення таких важливих завдань: гармонізація вітчизняного інформаційного законодавства з вимогами міжнародних актів, подолання прогалин щодо реалізації права на інформацію, удосконалення й розвиток інституту юридичної відповідальності за правопорушення в інформаційній сфері тощо.

6. За напрямами пізнавального процесу в галузі забезпечення інформаційної безпеки:

– професійна освіта;

– наукові дослідження;

– інформаційно-просвітницька діяльність.

Комплексність підходів до осягнення інформаційної безпеки зумовлює виділення особливої діяльності, що закладає інтелектуальні підвалини успішного національного інформаційного розвитку. Основними формами такої діяльності є профе-

сійна освіта та організація наукових досліджень у сфері інформаційної діяльності, що були безпосередньо визначені ст. 15, 16 однієї з попередніх редакцій Закону України «Про інформацію» (згідно з його останніми змінами і доповненнями від 02.12.2010) [250]. Доктриною ж інформаційної безпеки Російської Федерації організацію фундаментальних і прикладних наукових досліджень у галузі забезпечення інформаційної безпеки віднесено до основних функцій системи забезпечення інформаційної безпеки Російської Федерації, а зниження ефективності системи освіти та виховання, недостатня кількість кваліфікованих кадрів визнаються одним із внутрішніх джерел загроз інформаційній безпеці [89].

Високому рівню інформаційно-правової культури і професійної підготовки фахівців із забезпечення інформаційної безпеки відводиться одне з фундаментальних місць у системі гарантій інформаційної безпеки. В умовах реформування системи вищої освіти в Україні організація такої підготовки є складним завданням, виконанню якого сприятиме створення консолідованими зусиллями системи цільової підготовки й перепідготовки фахівців у різних галузях забезпечення інформаційної безпеки.

Зокрема до результатів такої діяльності належить створення напряму підготовки фахівців із вищою освітою – 170103 «Управління інформаційною безпекою» [249], яка здійснюється деякими провідними вищими навчальними закладами України. Прикладом міжнародної співпраці щодо перепідготовки фахівців є Концепція підготовки суддів і прокурорів із питань кіберзлочинності, розроблена Радою Європи в межах Проекту «Кіберзлочинність» та Лісабонською мережею Ради Європи з підготовки суддів протягом 2009 року [356].

Важливість усебічних наукових досліджень у нових сферах життєдіяльності держави і суспільства не викликає сумнівів. На сучасному етапі входження інформаційних відносин до сфери правового регулювання особливої актуальності набувають правові дослідження, гармонійним предметом яких є інформаційна безпека. З цього приводу слушна думка А. І. Марущака, який на-

голошує на доречності застосування класичних напрямів досліджень юридичної науки стосовно проблем, пов'язаних з інформаційною безпекою, а саме:

– науково-теоретичне обґрунтування доцільності правового регулювання суспільних відносин, що виникають із приводу інформаційної безпеки особи, суспільства, держави;

– визначення основних понять та категорій, які застосовуватимуться для унормування відповідних суспільних процесів;

– наукові розробки щодо повноважень суб'єктів суспільних інформаційно-безпекових відносин, форм і методів їх реалізації;

– дослідження питань юридичної відповідальності за правопорушення у сфері інформаційної безпеки [179, с. 37].

Інформаційно-просвітницька діяльність є втіленням такого засобу реалізації державної влади, як переконання, і загалом полягає в підвищенні рівня всіх складових інформаційної культури суспільства, особливо інформаційно-правової. Крім того, важливою складовою цієї діяльності є надання суспільству об'єктивної та всебічної інформації щодо чинників, які зумовлюють основні напрями державної політики, з метою формування консолідованої суспільної думки стосовно них. Так, серед напрямів державної політики у сфері інформаційної безпеки України окремо виділяється посилення інформаційно-просвітницької діяльності серед населення щодо забезпечення національної безпеки України в разі повноправного її партнерства з державами-членами ЄС та НАТО [247].

7. *Залежно від елементів змісту діяльності із забезпечення інформаційної безпеки:*

1) за об'єктами забезпечення інформаційної безпеки:

- розвиток і вдосконалення інформаційно-телекомунікаційної інфраструктури, недопущення доведення її до критичного рівня (захист критичної інформаційно-телекомунікаційної інфраструктури);

- забезпечення законного та ефективного використання національних інформаційних ресурсів (захист національних ін-

формаційних ресурсів від несанкціонованого втручання, інноваційне їх оновлення, впровадження новітніх технологій створення, оброблення та поширення інформації, формування відкритих державних інформаційних ресурсів і забезпечення доступу до них громадян);

- захист інформації (забезпечення якісних характеристик інформації – конфіденційності, цілісності та доступності тощо);

- захист свідомості суб'єктів (особи, групи осіб, суспільства) від деструктивного інформаційного впливу (створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей) [227; 247];

2) за суб'єктами забезпечення інформаційної безпеки:

- міжнародне забезпечення (міжнародне співробітництво в галузі забезпечення інформаційної безпеки, гарантування інформаційного суверенітету держави, сприяння задоволенню інформаційних потреб громадян за кордоном);

- державне забезпечення (діяльність державних організацій, спрямована на забезпечення інформаційної безпеки);

- недержавне забезпечення (діяльність громадських і недержавних комерційних організацій та окремих громадян (або інститутів громадянського суспільства), спрямована на сприяння державному забезпеченню інформаційної безпеки) [247];

3) за характером предмета діяльності із забезпечення інформаційної безпеки:

- протидія негативним інформаційним процесам і явищам (загрозам, небезпекам);

- сприяння посиленню позитивних інформаційних процесів (процесів розвитку суспільства);

- сприяння трансформації нейтральних інформаційних процесів у позитивні;

4) за складовими механізму протидії загрозам інформаційній безпеці:

- моніторинг інформаційної сфери (аналіз факторів впливу на інформаційну сферу, виявлення серед них загроз інформаційній безпеці);

- ранжування загроз (установлення пріоритетності напрямів державної діяльності з протидії загрозам інформаційній безпеці);

- профілактика і попередження негативного впливу загроз;

- нейтралізація загроз;

5) за характером здійснення державного впливу:

- безпосереднє створення необхідних умов життєдіяльності суб'єктів в інформаційній сфері;

- опосередкований вплив шляхом підвищення інформаційного потенціалу суб'єктів і сприяння їх самоорганізації;

6) за засобами забезпечення інформаційної безпеки:

- правове забезпечення (правова регламентація відносин в інформаційній сфері; контрольно-наглядова діяльність, зокрема шляхом нагляду за дотриманням законності в інформаційній сфері, а також ліцензування, сертифікації, експертизи та ін.);

- техніко-технологічне забезпечення (інженерно-технічне, матеріально-технічне, програмно-апаратне, криптографічне забезпечення тощо).

8. *Залежно від особливостей забезпечення доступу до інформації*:

1) за правовим режимом доступу до інформації:

- забезпечення режиму доступу до інформації з обмеженим доступом;

- забезпечення оптимального обміну відкритою інформацією;

- забезпечення належного розповсюдження публічної інформації;

2) за заходами із захисту секретної інформації:

- інженерно-технічне забезпечення;

- організаційно-правове забезпечення;

- оперативно-розшукове забезпечення;

- криптографічне забезпечення [246; 248].

Звичайно, наведена структуризація діяльності із забезпечення інформаційної безпеки не є вичерпною. Міждисципліна-

рний характер інформаційної безпеки, що охоплює технічні (технологічні), правові, психологічні аспекти, зумовлює надзвичайну складність і багаторівневість системних зв'язків складових забезпечення інформаційної безпеки. Усвідомлення особливостей кожної з них сприятиме процесам осягнення комплексності забезпечення інформаційної безпеки, визначенню тактичних і стратегічних напрямів діяльності у сфері забезпечення інформаційної безпеки, гармонізації національного інформаційного законодавства, що в сукупності створює важливі засади ефективної державної інформаційної політики [322].

2.3. Зміст державної діяльності із забезпечення інформаційної безпеки

Забезпечення інформаційної безпеки – широка, складна, різнопланова, об'єктивно необхідна діяльність. Державі як консолідуючому організатору суспільного життя, що має у своєму активі повний комплекс правових засобів, відводиться особлива роль у процесах забезпечення інформаційної безпеки. Значний внесок в усвідомлення особливостей державної діяльності із забезпечення інформаційної безпеки забезпечує розкриття її змістових характеристик на основі застосування діяльнісного підходу [318; 319].

Енциклопедичні джерела, відображаючи загальнонауковий аспект діяльності, визначають її як спосіб буття людини у світі, як здатність людини вносити зміни в дійсність. При цьому зміст діяльності розкривається за допомогою низки взаємопов'язаних елементів, які становлять незмінну основу діяльності, зберігають її властивості навіть за умов зовнішніх змін, надають діяльності рис сталості [74, с. 89].

Цими елементами є: об'єкт і предмет, на який спрямована діяльність; суб'єкт із його потребами й інтересами; мета, відповідно до якої перетворюється предмет; засоби та методи досягнення мети, принципи і результати діяльності. Саме їх доцільно

розглядати як інтегруючу основу змісту діяльності із забезпечення інформаційної безпеки.

Слід також зазначити, що названі елементи в різних комбінаціях утворюють інші конструкції, які достатньо активно використовуються в наукових дослідженнях сфери національної та інформаційної безпеки, а саме: суб'єкти в поєднанні із засобами й заходами із застосування цих засобів найчастіше асоціюються із системою забезпечення; мета і відповідні їй методи й засоби відображають механізм забезпечення; методи, способи та засоби визначають шляхи забезпечення тощо.

1. *Об'єкт забезпечення інформаційної безпеки.* Об'єкт безпеки є однією з фундаментальних категорій теорії безпеки, що визначає змістову спрямованість безпеки, її конкретного виду або складової.

З огляду на інформаційну безпеку як особливий елемент системи національної безпеки важливим є встановлення співвідношення об'єктів інформаційної безпеки з об'єктами безпеки вищого порядку – національної, чому як вітчизняним законодавством, так і наукою не приділяється належна увага.

Так, Доктрина інформаційної безпеки України лише розкриває відповідні особливості об'єктів національної безпеки, визначених Законом України «Про основи національної безпеки» як людина і громадянин, суспільство, держава, в ракурсі інформаційної безпеки, безпосередньо не конкретизуючи її об'єкти і користуючись при цьому конструкцією «життєво важливі інтереси в інформаційній сфері».

Стосовно особи ці інтереси виявляються в забезпеченні конституційних прав і свобод людини на збирання, зберігання, використання і поширення інформації; недопущенні несанкціонованого втручання в зміст, процеси оброблення, передавання та використання персональних даних; захищеності від негативного інформаційно-психологічного впливу.

Щодо суспільства – у збереженні й примноженні духовних, культурних і моральних цінностей Українського народу;

забезпеченні суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; формуванні й розвитку демократичних інститутів громадянського суспільства.

Стосовно держави – в недопущенні інформаційної залежності, інформаційної блокади України, інформаційної експансії інших держав та міжнародних структур; ефективній взаємодії органів державної влади й інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері; побудові й розвитку інформаційного суспільства; забезпеченні економічного та науково-технологічного розвитку України; формуванні позитивного іміджу України; інтеграції України у світовий інформаційний простір [247].

Дещо інший підхід обрано законодавцем у Концепції Національної програми інформатизації, прийнятій у 1998 році, яка окреслює об'єкти інформаційної безпеки як елементи інформаційної інфраструктури країни, зокрема: інформаційні ресурси, канали інформаційного обміну й телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж [252].

Наукові інтерпретації об'єктів забезпечення інформаційної безпеки більш конкретизовані, ніж нормативні, проте характеризуються значним плюралізмом підходів.

Так, В. І. Полевий об'єктами системи забезпечення інформаційної безпеки визначає: 1) засоби комунікації та масиви інформації, відображені на матеріальних носіях (технічна складова інформаційної безпеки); 2) свідомість особи, групи осіб або масова свідомість (психологічна складова); 3) інформація з обмеженим доступом, яка є критично важливою для держави або інших суб'єктів (змістова складова) [236].

Схожої позиції дотримується О. М. Солодка, яка до елементів захисту інформаційної безпеки України в процесі євроатлантичної інтеграції, які, по суті, і є об'єктами інформаційної безпеки, відносить: 1) інформаційні права суб'єктів; 2) інформацію з

обмеженим доступом; 3) інформаційний простір; 4) системи і засоби передавання й зберігання інформації [286].

А. Б. Качинський об'єктами інформаційної безпеки вважає інформацію та її інфраструктуру [125, с. 20].

В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський визначають об'єкти системи забезпечення інформаційної безпеки України через: 1) інтереси органів державного управління в інформаційній сфері; 2) систему органів державного управління, а також їх компетентних осіб і відносини між ними (суспільні відносини в інформаційній сфері); 3) власне систему забезпечення інформаційної безпеки України [162, с. 162].

Наведене вище свідчить про відсутність загальновизнаного уявлення щодо об'єктів забезпечення інформаційної безпеки й необхідність певного переосмислення наявних підходів, що може бути здійснено на основі таких теоретичних позицій.

По-перше, система національної безпеки й система забезпечення національної безпеки не є тотожними поняттями і, відповідно, об'єкти національної безпеки та об'єкти забезпечення кожної з її складових, зокрема інформаційної, повинні розглядатися як різнопорядкові явища. Виходячи з гуманітарної парадигми національної безпеки та певної суб'єктивності поняття «безпека» [321], об'єкти національної безпеки, визначені як особа, суспільство й держава, сприймаються як родові щодо об'єктів забезпечення кожної складової національної безпеки. З цієї позиції підхід до розкриття об'єктів забезпечення інформаційної безпеки, використаний у Доктрині інформаційної безпеки України, не виглядає як недолік, адже в сутності безпека об'єкта виявляється через захищеність його найважливіших якостей (якостей його структурних складових), якими в українському законодавстві виступають життєво важливі інтереси.

По-друге, об'єктом забезпечення інформаційної безпеки є будь-яка соціальна, технічна або соціотехнічна система, функціонування якої визначально залежить від її інформаційної інфраструктури.

По-третє, загальним об'єктом забезпечення інформаційної безпеки може розглядатися сама інформаційна безпека як система умов функціонування і розвитку суб'єктів в інформаційній сфері. Тоді конкретизованими об'єктами забезпечення інформаційної безпеки виступатимуть об'єкти (явища) матеріального й нематеріального світу, які повинні створювати або забезпечувати оптимальні умови функціонування суб'єктів в інформаційному середовищі. Їх доцільно розглядати в правовому, психологічному та техніко-технічному контекстах, тобто відповідно до сучасного уявлення про складові інформаційної безпеки.

Отже, загальними об'єктами національної та інформаційної безпеки є особа, суспільство, держава. Тоді узагальненими об'єктами забезпечення інформаційної безпеки можна уважати інформаційну інфраструктуру (держави, суспільства), яка має технічні й правові компоненти, і свідомість (особи, суспільства), що загалом інтерпретується таким чином:

1) технічні компоненти інформаційної інфраструктури: технічні канали інформаційного обміну й телекомунікації, а також технічні системи оброблення та збереження інформації (інженерно-технічний контекст);

2) правові компоненти інформаційної інфраструктури: інформаційні права та обов'язки суб'єктів; правові механізми забезпечення функціонування інформаційних ресурсів, телекомунікаційних систем і мереж; правовий порядок збереження конфіденційності, цілісності та доступності інформації (правовий контекст);

3) свідомість особи, групи осіб, суспільства (психологічний клімат у національному інформаційному просторі); змістові характеристики соціально важливої інформації (психологічний контекст).

Розглядаючи об'єкти, не можна оминути увагою *предмет забезпечення інформаційної безпеки*, оскільки саме ним зумовлюються окремі напрями діяльності суб'єктів забезпечення інформаційної безпеки, які прийнято називати їхніми функціями (функціями системи забезпечення інформаційної безпеки).

У системі «об'єкт – предмет діяльності» предмет – це та складова або компонент об'єкта діяльності (певна цілісність, виділена з об'єкта діяльності), на яку суб'єкт спрямовує свою діяльність і яка підлягає трансформації.

Як уже зазначалося, об'єктом забезпечення інформаційної безпеки є власне інформаційна безпека як сукупність різноманітних умов життєдіяльності суб'єктів в інформаційній сфері. Процеси, якими створюються ці умови, можуть мати як позитивний (конструктивний), так і негативний (деструктивний) характер. Відповідно, виокремлюються дві сфери предметної спрямованості діяльності із забезпечення інформаційної безпеки: 1) сприяння позитивним процесам; 2) протидія негативним процесам.

Негативні процеси у своїй сутності становлять загрози (небезпеки, виклики, ризики тощо), які гальмують розвиток або сприяють деградації, у той час як позитивні процеси, що можуть сприйматися через нормативно-правову конструкцію «життєво важливі інтереси», стимулюють і забезпечують розвиток.

Проте слід звернути увагу на деякі важливі діалектичні особливості цих явищ. Так, загрози або інші негативні чинники, що не спричиняють дестабілізуючого ефекту, але усвідомлюються суб'єктом, є стимулом його еволюції в напрямі набуття якостей, які протиставляються негативному впливу, виробляючи тим самим певний рівень імунітету. І навпаки, наявність лише позитивних процесів або тривала відсутність окремих загроз може призвести до послаблення та атрофії захисних механізмів. Це означає, що оптимальне середовище функціонування суб'єктів, зокрема інформаційне, повинно сприйматися не ідеалістично, а як об'єктивно необхідна сукупність позитивних і негативних недестабілізуючих чинників, які загалом забезпечують бажаний розвиток. Така позиція підкреслює обов'язкову наявність синергетичної складової процесу забезпечення інформаційної безпеки, що повною мірою відповідає тенденціям розвитку сучасного суспільства (громадянського, інформаційного), яке ґрунтується на самоорганізації.

У наукових джерелах досить детально розкриті питання класифікації та змісту загроз і життєво важливих інтересів у сферах забезпечення національної та інформаційної безпеки. Серед українських дослідників їх широко розглядали А. Л. Баланда, В. Ю. Боданович, В. П. Горбулін, А. Б. Качинський, Б. А. Кормич, В. А. Ліпкан, Г. В. Новицький, В. В. Остроухов та інші.

Знайшли вони своє закріплення та змістове наповнення і на концептуально-доктринальному рівні законодавства сучасних держав, а також у міжнародних актах. У вітчизняному законодавстві загрози й життєво важливі інтереси в інформаційній сфері та похідні від них «напрями забезпечення національної (інформаційної) безпеки», «напрями державної політики у сфері інформаційної безпеки», «напрями державної інформаційної політики» прямо чи опосередковано відображені в законах України «Про основи національної безпеки», «Про стратегію національної безпеки України», «Про основи державної політики у сфері науки і науково-технічної діяльності», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про Концепцію Національної програми інформатизації», «Про Національну програму інформатизації», «Про інформацію», «Про доступ до публічної інформації», а також у Доктрині інформаційної безпеки України.

2. *Суб'єкти забезпечення інформаційної безпеки.* З філософської точки зору суб'єкт діяльності – це носій діяльності, те, що уособлює активне творче начало діяльності. У контексті забезпечення безпеки важливим є розгляд суб'єкта діяльності в нерозривному зв'язку з тим, на що саме спрямована ця діяльність, тобто з об'єктом діяльності, оскільки в реальності суб'єкти й об'єкти забезпечення безпеки можуть виступати одночасно і тим, й іншим.

Суб'єкт забезпечення безпеки – одна з основних категорій, що використовується для розкриття змісту системи забезпечення як національної, так і інформаційної безпеки. Традиційно йому приділяється багато уваги на нормативно-правовому рівні,

оскільки саме право в сучасній правовій державі є засобом визначення повноважень суб'єктів державної діяльності та окреслення сфери їх компетенції.

Теорія національної безпеки відносить до суб'єктів забезпечення всі державні та суспільні інституції, які є учасниками процесу забезпечення національної безпеки, а саме: апарат держави як систему державних органів, органи місцевого самоврядування, громадян та їх об'єднання. З цього переліку виокремлюються суб'єкти, які наділені державно-владними повноваженнями, і суб'єкти, які ними не наділені, хоча в деяких випадках можуть мати певний обсяг делегованих державно-владних повноважень.

На думку М. Б. Левицької, це інтерпретується таким чином:

1) суб'єкти, діяльність яких безпосередньо підпорядкована завданням забезпечення національної безпеки, як у комплексі, так і окремим із них (Рада національної безпеки й оборони України, правоохоронні та інші державні виконавчі органи спеціальної компетенції);

2) суб'єкти, для яких така діяльність є одним з основних, але не єдиним напрямом (вищі органи законодавчої, виконавчої та державної влади);

3) суб'єкти, для яких участь у забезпеченні національної безпеки не є основною діяльністю (всі інші державні й громадські організації) [157, с. 66].

Тобто формально виділяються дві взаємодоповнюючі складові забезпечення національної безпеки: державне забезпечення і недержавне забезпечення.

Аналогічний підхід доцільно застосовувати і щодо розгляду суб'єктів забезпечення інформаційної безпеки, причому виділення суб'єктів недержавного забезпечення є особливо актуальним, зважаючи на складність, динамічність та синергетичність процесів інформаційного розвитку суспільства. Як зазначає колектив авторів під керівництвом Ю. С. Шемшученка та І. С. Чижа, «політика інформаційної безпеки має реалізовувати-

ся як системою інститутів публічної влади, так і інститутами громадянського суспільства, до компетенції яких належить вирішення питань створення безпечних умов функціонування і розвитку інформаційної сфери» [244, с. 79].

Крім того, в умовах сучасних світових глобалізаційних процесів, коли і національна, і тим більше інформаційна безпека держави розглядаються як явища наднаціонального (наддержавного) характеру, модель ефективного виключно самостійного забезпечення власної інформаційної безпеки окремою державою виглядає недосконалою. Сьогодні науковці наголошують на необхідності формування системи забезпечення міжнародної безпеки, а значну частину концептуальних положень національних законодавств провідних країн світу у сфері безпеки, зокрема інформаційної, визначають домовленості, закріплені відповідними міжнародними актами, які є результатом діяльності міжнародних організацій.

Отже, серед суб'єктів забезпечення інформаційної безпеки узагальнено можна виділити три групи:

– міжнародні організації;

– держава в особі державних організацій;

– недержавні організації, громадяни та їх об'єднання.

Звичайно, держава, яка безпосередньо здійснює державне забезпечення інформаційної безпеки, посідає особливе місце серед цих суб'єктів, оскільки тільки вона, виступаючи повноважним представником свого народу, у тісній взаємодії з міжнародними організаціями та інститутами громадянського й інформаційного суспільства здатна сформувати цілісну національну політику забезпечення інформаційної безпеки, що враховуватиме наявні та потенційні інтереси суспільства й особливості свого міжнародного становища.

Кожна державна організація в межах своєї діяльності, реалізуючи функції держави, тією чи іншою мірою виступає суб'єктом державного забезпечення інформаційної безпеки. При цьому є система державних органів, для яких окремі напрями забезпечення інформаційної безпеки є безпосередньою

функцією. В Україні це Служба безпеки України, Служба зовнішньої розвідки України, Міністерство оборони України, Міністерство закордонних справ України, Державна служба спеціального зв'язку та захисту інформації України, Національна комісія з питань регулювання зв'язку України, Національна експертна комісія України з питань захисту суспільної моралі, Державна адміністрація зв'язку Міністерства транспорту та зв'язку України, Державна служба України з питань захисту персональних даних, Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України, Національна рада України з питань телебачення і радіомовлення, а також Головне управління з питань безпекової та оборонної політики, Головне управління забезпечення доступу до публічної інформації, Управління з питань комунікацій Адміністрації Президента України та інші.

Серед міжнародних організацій, рішення яких відіграють важливу роль у формуванні системи забезпечення інформаційної безпеки як регіонального та світового масштабу, так і окремих держав, доцільно виділити: Європейський Союз (ЄС); Організацію Об'єднаних Націй (ООН); Організацію Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО); Шанхайську організацію співробітництва (ШОС); Євразійське економічне співтовариство (ЄврАзЕС); Північноатлантичний Альянс (НАТО).

Недержавне забезпечення інформаційної безпеки може здійснюватися численними недержавними інституціями, зокрема: засобами масової інформації; провайдерами телекомунікаційних послуг; комерційними підприємствами, які надають послуги з технічного захисту інформації; різноманітними об'єднаннями громадян, які здійснюють громадський контроль державного забезпечення інформаційної безпеки та сприяння йому тощо.

3. *Мета забезпечення інформаційної безпеки.* Мета є постійним фактором, обов'язковим і необхідним елементом будь-якої цілеспрямованої діяльності. З одного боку, мета діяльності

може розглядатися як вихідний, детермінуючий компонент не лише змісту, а й структури діяльності. З іншого боку, вона зумовлюється низкою зовнішніх факторів, наявних у рамках соціального середовища, передусім потребами та інтересами. Водночас мета діяльності формується під впливом інших факторів: режиму законності, стану правопорядку, політичної обстановки або економічної ситуації в країні, рівня правової культури тощо [74, с. 97].

Рівень визначеності мети може бути різним і залежить від характеристик суб'єкта, особливостей сфери його діяльності. Очевидно, що мета масштабної консолідуючої діяльності, якою є забезпечення національної безпеки, має найвищий рівень узагальненості й сталості, а мета забезпечення інформаційної безпеки як складової національної більш конкретизована і розкривається завданнями діяльності, що постають на певному етапі розвитку і змінюються з часом.

На загальнотеоретичному рівні мета забезпечення інформаційної безпеки також може розглядатися достатньо абстрактно, зокрема як досягнення такого стану інформаційної безпеки, який забезпечує оптимальне задоволення інформаційних потреб й інтересів суб'єктів. Або ж, у соціологічному аспекті, – як формування системи суспільних відносин, у межах яких належним чином задовольняються національні інтереси та об'єктом яких є інформація, інформаційна діяльність, інформаційна інфраструктура тощо.

Мета забезпечення національної безпеки України визначається пріоритетами національних інтересів (ст. 6 Закону України «Про основи національної безпеки»), що розкривають конституційну модель України (ст. 1 Конституції України) як суверенної і незалежної, демократичної, соціальної, правової держави.

Натомість мета забезпечення інформаційної безпеки України опосередковано відображається в пріоритетах національних інтересів, але безпосередньо закріплена Доктриною інформаційної безпеки України як «створення в Україні розвиненого національного інформаційного простору і захист її інформацій-

ного суверенітету» [247]. Проте таке формулювання дещо зміщує акцент із соціально-гуманітарної складової, пріоритетної для національної безпеки (забезпечення реалізації прав, свобод та життєво важливих інтересів, особливо інтелектуального, духовного й культурного розвитку людини та громадянина), на технологічну і не відбиває синергетичні та субсидіарні особливості інформаційної безпеки, її взаємозв'язки з інформаційним суспільством.

Із цих позицій більш досконалою виглядає інтерпретація мети забезпечення інформаційної безпеки на основі Окінавської хартії глобального інформаційного суспільства та відповідних їй загальних положень Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» через пріоритетність розбудови орієнтованого на інтереси людей, відкритого для всіх і спрямованого на розвиток інформаційного суспільства, в якому кожен має можливість створювати і накопичувати інформацію та знання, вільно їх отримувати, користуватися й обмінюватися ними, тим самим у повній мірі реалізовувати свій потенціал, сприяючи суспільному й особистому розвитку та підвищуючи якість життя [207; 255].

Подальша деталізація мети забезпечення інформаційної безпеки може здійснюватись через основні завдання, що стоять перед Україною на сучасному етапі розвитку, до яких в інформаційній сфері належать:

– інформатизація процесів управління державою;

– формування доступних національних інформаційних ресурсів;

– інтеграція у світовий інформаційний простір;

– збереження національної ідентичності та популяризація національної культури;

– розвиток інтелектуального потенціалу країни;

– створення позитивного морально-психологічного клімату в національному інформаційному просторі;

– формування позитивного іміджу України на світовій арені;

– протидія кіберзлочинності та кібертероризму тощо.

4. *Засоби й методи забезпечення інформаційної безпеки.* Вибір методів і засобів у будь-якій сфері діяльності загалом визначається метою та завданнями. Забезпечення інформаційної безпеки є комплексним видом діяльності, що зумовлює наявність у її арсеналі широкого кола методів і засобів, притаманних різним галузям, сферам діяльності. Ці засоби та методи, визначаючи один одного та об'єднуючись на різних рівнях забезпечення в системи, утворюють механізми забезпечення інформаційної безпеки.

Концепції систематизації механізмів забезпечення інформаційної безпеки можуть бути різними. Так, у сфері, окресленій серією стандартів ISO/IEC 27000, яку прийнято називати управлінням інформаційною безпекою, традиційно виділяється декілька рівнів: 1) фізичний; 2) програмно-технічний; 3) управлінський; 4) технологічний; 5) рівень користувача; 6) мережевий; 7) процедурний [361]. Ці рівні відображають визнану систему забезпечення інформаційної безпеки окремих організацій (органів, підприємств, установ тощо) та створення безпечних каналів обміну інформацією між ними, проте не охоплюють всієї багатоаспектності інформаційної безпеки, оскільки згадана діяльність орієнтована переважно на захист інформації, необхідної окремим суб'єктам у процесі здійснення ними певних видів діяльності.

Для загального осягнення системи засобів та методів забезпечення інформаційної безпеки пропонується розглядати їх крізь гіпотетичну трирівневу модель:

1) рівень загального сприяння (регулятивний рівень);

2) рівень індивідуального сприяння (рівень стимулювання самозахисту суб'єктів);

3) рівень захисту (охоронний рівень).

Першому рівню відповідають методи і засоби, які стосовно другого й третього рівнів мають загальний характер. Вони притаманні багатьом сферам діяльності (політичній, правовій, економічній, освітній, науково-технологічній та ін.) і використовуються для створення загальних умов задоволення потреб та

інтересів суб'єктів в інформаційній сфері, що загалом виражається в розвитку інформаційної інфраструктури держави та національних інформаційних ресурсів, а також загальному інтелектуальному і культурному розвитку населення.

Другий рівень передбачає методи й засоби освітньо-виховного індивідуального впливу, спрямованого на формування здатностей самостійного забезпечення власної інформаційної безпеки, зокрема підвищення рівня культури використання засобів оброблення інформації, критичного ставлення до інформації, а також сприяння розвитку механізмів внутрішньоособистісного психологічного захисту.

Третьому рівню відповідають спеціальні методи й засоби, які загалом утворюють: механізми організаційно-правового і технічного збереження якісних характеристик інформації (захисту інформації), механізми протидії маніпулюванню свідомістю суспільства шляхом надання викривленої, недостовірної, неповної інформації або використання сугестивних технологій і, зокрема, нейролінгвістичного програмування [299]; механізми контролю застосування спеціальних методів та засобів.

Запропоноване вище є лише альтернативним виміром, який не заперечує наявних варіацій систематизації засобів та методів, що використовуються у сфері інформаційної безпеки.

Їх систему можна інтерпретувати й іншим способом: 1) правові; 2) управлінсько-організаційні; 3) інформаційно-аналітичні, прогностичні; 4) психологічного захисту особистості; 5) технічного й криптографічного захисту інформації тощо.

Пріоритетність правових засобів і методів є домінантою сучасної правової держави. Право як єдиний універсальний соціальний регулятор охоплює і сферу державного забезпечення інформаційної безпеки. Адже саме правовими механізмами в сучасній державі здійснюється розмежування повноважень суб'єктів забезпечення інформаційної безпеки та встановлюється порядок використання ними спеціальних засобів і методів.

Універсальна класифікація правових засобів (здійснена безвідносно до сфери правової діяльності), яка дозволяє на за-

гальнотеоретичному рівні охопити правову складову будь-якої соціально значущої діяльності, зокрема забезпечення інформаційної безпеки, запропонована С. С. Алексєєвим. До них належать:

а) явища-регулятори, які є основою і механізмом правового регулювання (норми, правоположення практики, індивідуальні приписи, права та обов'язки);

б) явища правової форми – нормативні та індивідуальні акти;

в) явища правової діяльності – правотворчість, правозастосування, тлумачення;

г) явища суб'єктивної сторони правової дійсності – правосвідомість, суб'єктивні елементи правової культури, правова наука [4].

Щодо методів правового регулювання, то найбільш поширена класифікація, яка здійснюється за характером впливу права на регульовані суспільні відносини. За цим критерієм прийнято виділяти два методи: імперативний та диспозитивний.

Імперативний метод застосовується для врегулювання суспільних відносин, що базуються на принципах субординації, і включає три способи: дозвіл, зобов'язання, заборону. Диспозитивний метод застосовується для врегулювання суспільних відносин, які потребують координації інтересів суб'єктів [171, с. 379]. На відміну від імперативного методу, який установлює чіткі варіанти дозволеної, забороненої або необхідної поведінки, диспозитивний метод полягає у визначенні меж, у яких учасники відносин самостійно обирають варіанти своєї взаємної поведінки.

Як спеціальні механізми організаційно-правового забезпечення інформаційної безпеки можуть розглядатися механізми регламентації та контролю окремих специфічних видів діяльності, такі як ліцензування, сертифікація, експертиза, а також державна та міжнародна стандартизація, яка широко використовується в інформаційній сфері.

Проте універсальність правових механізмів не робить їх ідеальними і всеосяжними. Так, сьогодні не достатньо охопле-

ною регулятивними та охоронними функціями права є так звана кібернетична сфера – сфера суспільних відносин, пов'язана з обробленням електронних комп'ютерних даних із використанням глобальних інформаційно-телекомунікаційних мереж, яка несе значне коло загроз інформаційній безпеці. Серед них кіберзлочинність і кібертероризм, які мають високий рівень латентності, а тому не піддаються відповідному державному реагуванню.

За офіційними даними Міністерства внутрішніх справ України за 2010–2012 роки, злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку в Україні становлять лише соті частки відсотка в загальному обсязі зареєстрованих злочинів, хоча практично кожен громадянин, який активно використовує здобутки інформаційно-телекомунікаційних технологій, відчуває на собі наслідки такого виду правопорушень. Таким чином, набуття кіберсферою особливого суспільного значення зумовлює необхідність віднесення частини суспільних відносин у ній до сфери правового регулювання та відповідне переосмислення і вдосконалення правових механізмів.

Загалом оптимальність глибини й обсягу правового регулювання, адекватність вибору правових засобів і методів безпосередньо визначає ефективність соціально значущих проявів інформаційної діяльності і, як наслідок, якість організаційного підґрунтя забезпечення інформаційної безпеки.

Не менш важливе місце в системі засобів і методів державного забезпечення інформаційної безпеки посідає спектр методів управління та організації діяльності, які в поєднанні з правовими методами й засобами створюють механізми реалізації державної влади. У загальному вигляді до них належать переконання, примус, стимулювання.

Зважаючи на синергетичність процесів розвитку інформаційного і громадянського суспільства, окремо слід відмітити метод переконання, який закладає основи як державного, так і недержавного забезпечення інформаційної безпеки. Переконання, в рамках якого здійснюється цілеспрямований вплив на сві-

домість людей шляхом роз'яснення їх прав та обов'язків, привернення уваги, підвищення зацікавленості, поєднання соціальних інтересів конкретної особи з інтересами суспільства і держави, можна вважати одним з головних ресурсів забезпечення інформаційної безпеки.

Практичне застосування цього методу у сфері інформаційної безпеки є багатоваріантним. Забезпечення режимів доступу до інформації багато в чому залежить саме від переконання. Зокрема дуже часто дослідники пов'язують причини витоку таємної й конфіденційної інформації безпосередньо з особистими якостями осіб, які відповідальні за її збереження та нерозповсюдження. Високоефективним є метод переконання і щодо реалізації вимог законодавства в інформаційній сфері, захисту інформаційних прав і свобод людини, захисту моральності тощо. Крім того, методом переконання здійснюється інформаційне забезпечення державної політики загалом, яке також є предметом інформаційної безпеки держави [141].

Застосування державного примусу більш актуальне щодо відповідальності за правопорушення в інформаційній сфері, фізичного захисту об'єктів інформаційної інфраструктури і носіїв інформації з обмеженим доступом.

Певні аспекти інформаційної безпеки виступають широким полем для застосування методу заохочення. Окрім суто внутрішньоапаратного застосування з метою заохочення співробітників або посадових осіб, величезне значення має зовнішній напрям. Він полягає в заохоченні діяльності фізичних та юридичних осіб, у результаті чого поліпшуються параметри і характеристики інформаційних відносин [141].

На відміну від правових та управлінських, методи та засоби технічного й психологічного забезпечення інформаційної безпеки мають вужчу сферу спрямованості, однак, використовуючись у процесі управління як допоміжні засоби, часто визначають його ефективність.

Серед технічних (технологічних) засобів та методів виокремлюються: засоби інформатизації (автоматизації) процесів ор-

ганізації та управління (новітні інформаційно-телекомунікаційні технології, що використовуються для оптимізації управління); засоби та методи технічного (фізичного, апаратного, програмного), криптографічного захисту інформації.

Психологічні механізми державного забезпечення інформаційної безпеки загалом зводяться до створення сприятливого морально-психологічного клімату в інформаційному просторі, виявлення та нейтралізації джерел деструктивного психологічного впливу, а також освітньо-виховної діяльності, спрямованої на формування певних утворень (форм захисту) психіки особистості, необхідних для індивідуальної захисної поведінки [70, с. 117; 90, с. 200].

Очевидно, що методологія забезпечення інформаційної безпеки повинна включати і методи, які дозволяють здійснювати аналітичні й прогностичні функції й на основі отриманих результатів формувати тактичні та стратегічні завдання системи державного забезпечення інформаційної безпеки. Серед них: методи опису, класифікації, дослідження причинових зв'язків, різноманітні методи моделювання оцінки загроз та небезпек, метод критичних сценаріїв, метод дихотомії, методи аналізу інформаційних ризиків (кількісний та якісний аналіз, факторний аналіз тощо) [161, с. 227–231].

5. *Принципи забезпечення інформаційної безпеки.* Принципи будь-якої діяльності людини відіграють важливу роль, оскільки встановлюють її вихідні, основоположні засади. Забезпечення інформаційної безпеки не є винятком. Сьогодні до нього висуваються особливі вимоги щодо відповідності не тільки принципам, притаманним власне сфері національної та інформаційної безпеки, а й конституційним принципам розбудови держави, принципам становлення сучасного суспільства.

У рамках діяльнісного підходу важливим є фокусування уваги на принципах, що відображають концепцію забезпечення інформаційної безпеки як комплексного виду діяльності в контексті розбудови правової держави, громадянського та інформаційного суспільства, а також глобалізаційних й інтеграційних процесів. Їх можна поділити на дві групи.

Першу групу становлять принципи, які відображають загальносистемні засади державної політики забезпечення інформаційної безпеки:

– комплексність підходів до забезпечення інформаційної безпеки;

– оптимальність системи забезпечення інформаційної безпеки;

– всебічна виваженість державної політики інформаційної безпеки;

– єдність та цілісність законодавчих підходів до забезпечення інформаційної безпеки;

– об'єктивність оцінки загроз та адекватність і своєчасність заходів із забезпечення інформаційної безпеки;

– чітке розмежування повноважень та взаємодія органів державної влади в забезпеченні національної безпеки;

– використання в інтересах країни міждержавних систем та механізмів міжнародної колективної безпеки.

Останнє ґрунтується на системі принципів міжнародної інформаційної безпеки, яка сьогодні активного формується.

До другої групи належать принципи, що закладають правові та демократичні основи діяльності із забезпечення інформаційної безпеки і на фоні сучасних перетворень суспільства поступово починають привертати більшу увагу дослідників інформаційної сфери [105]:

– свобода збирання, зберігання, використання та поширення інформації;

– гарантованість достовірності, повноти й неупередженості інформації;

– доступність інформації та законність обмеження доступу до інформації;

– інформаційна рівність;

– збалансованість особистих, суспільних і державних інтересів в інформаційній сфері;

– невідворотність юридичної відповідальності за правопорушення в інформаційній сфері та адекватність її міри;

– гармонійність національного і міжнародного законодавства в інформаційній сфері;

– пріоритетність національної інформаційної продукції;

– взаємна відповідальність особи, суспільства й держави;

– гласність і демократичний контроль забезпечення інформаційної безпеки тощо.

Окремо доцільно виділити низку принципів, що стосуються забезпечення інформаційно-психологічної безпеки. Характер деяких із них достатньо суперечливий, проте вони в майбутньому можуть набути законодавчого закріплення, чому вже є реальні підтвердження [257]:

– державна монополія на розроблення й виробництво спеціальних засобів інформаційно-психологічного впливу;

– законність використання спеціальних засобів інформаційно-психологічного впливу;

– обов'язковість участі громадських організацій у діяльності із забезпечення інформаційно-психологічної безпеки;

– організованість міжнародного співробітництва у сфері забезпечення інформаційно-психологічної безпеки;

– скоординованість діяльності органів державної влади і громадських об'єднань щодо забезпечення інформаційно-психологічної безпеки;

– захищеність традиційних підвалин суспільства й суспільної моральності.

6. *Результат забезпечення інформаційної безпеки.* Очевидно, що результат діяльності із забезпечення інформаційної безпеки має корелюватися із самою інформаційною безпекою, а точніше – її станом на момент оцінки результатів, інакше ця діяльність утрачає сенс.

Необхідною і логічною вбачається оцінка стану забезпечення інформаційної безпеки на підставі положень законодавства, що визначають мету, об'єкти, напрями забезпечення інформаційної безпеки, а також життєво важливі інтереси особи, суспільства, держави в інформаційній сфері.

Ця оцінка має водночас характер практичного і науково-теоретичного пізнання і повинна ґрунтуватись на таких методологічних принципах, як об'єктивність, реалістичність, усебічність і комплексність аналізу тощо. Однак реалізація цих принципів вимагає розроблення обґрунтованих методичних підходів і прийомів визначення реального стану та перспектив розвитку суспільних відносин в інформаційній сфері, зокрема у забезпеченні інформаційної безпеки, яких наразі немає.

Слід зазначити, що в науковому світі активізувалася робота з оцінювання рівня інформаційної безпеки із застосуванням математичних методів. Проте наявні моделі, методи і методики, які ґрунтуються на інформації з відкритих джерел, потребують розвитку і вдосконалення [226; 334]. Навіть у практично орієнтованій, стандартизованій сфері управління інформаційною безпекою комплексній оцінці результатів управління не приділяється увага.

Актуальним науковим і практичним завданням у сфері інформаційної безпеки залишається формування загальновизнаних підходів до визначення оптимальних моделей і шляхів її забезпечення на основі виявлення найважливіших якісних і кількісних властивостей та параметрів цього явища. Важливість такого завдання підтверджується і вітчизняним законодавством, яке визначає розроблення й упровадження системи індикаторів інформаційного розвитку суспільства та узгодження їх із міжнародними стандартами і методологією одним з основних напрямів розвитку інформаційного суспільства в Україні [187; 255].

Певною мірою вирішенню цього завдання можуть сприяти методи критеріального аналізу, які все частіше використовуються в дослідженнях явищ соціальної сфери [323; 324].

У міжнародній практиці поширена оцінка рівня розвитку інформаційного суспільства або його структурних елементів, що опосередковано відображає і стан інформаційної безпеки, адже він безпосередньо залежить від здатностей та можливос-

тей суб'єктів інформаційних відносин. Оцінювання здійснюється на основі е-індексів, вибір та методика побудови яких визначається обраними державою пріоритетами. До основних індикаторів експерти включають, зокрема, індикатори стану доступу до телекомунікаційної інфраструктури (радіо, телебачення, телефону, персональних комп'ютерів, інтернету), як населення загалом, так і певних організацій (освітніх закладів, різноманітних установ, державних органів тощо).

Найбільш поширені е-індекси: цифрової спроможності або цифрової перспективи (Digital Opportunity Index – DOI), цифрового доступу (Digital Access Index – DAI), мережевої готовності (The World Economic Forum's Networked Readiness Index – NRI), інформаційного суспільства (Informational Society Index – ISI). За цими індексами Україна посідає далеко не перші місця, що свідчить про неблизькі перспективи високого рівня інформаційної безпеки в широкому її розумінні [71].

Отже, інформаційна безпека як результат комплексної діяльності і як стан оптимального функціонування й розвитку суб'єктів в інформаційній сфері потребує комплексної оцінки через систему показників інформаційної безпеки – найбільш значущих параметрів, що надають загальне уявлення щодо інформаційної системи держави і суспільства, її стійкості, ефективності, здатності до розвитку тощо. Систему показників доцільно розділити на два логічних блоки: 1) критерії та показники, що відображають технологічну сторону інформаційної безпеки (рівень розвитку й захищеності інформаційної інфраструктури); 2) критерії та показники, що відображають рівень інформаційного розвитку суб'єктів (зокрема держави, суспільства), а також наявні та потенційні можливості забезпечення власної інформаційної безпеки.

Належне місце в комплексній оцінці забезпечення інформаційної безпеки повинна посісти правова оцінка, яка відображатиме рівень реалізованості правових засад інформаційної безпеки особи, суспільства, держави, тобто ефективність наявних правових механізмів безпечного функціонування суб'єктів

в інформаційній сфері. На загальному рівні правову оцінку можна здійснювати через стан законності та правопорядку в інформаційній сфері, передусім за допомогою показників, що відображають:

– правовий режим інтелектуальної власності («ноу-хау», патенти, промислові зразки, рівень промислового шпигунства) [291];

– стан реалізації інформаційних прав (випадки обмеження свободи слова, безпідставного віднесення інформації до конфіденційної, викривлення та приховування інформації);

– рівень інформаційно-правової культури;

– статистику всіх видів правопорушень в інформаційній сфері, передбачених національним законодавством;

– статистику звернення до омбудсмена з питань порушення права на інформацію;

– стан проблем, пов'язаних із дотриманням конституційних прав і свобод громадян у сфері духовного життя та інформаційної діяльності тощо [323].

Отже, змістовий аналіз державного забезпечення інформаційної безпеки дозволяє дійти висновку, що інформаційна безпека як об'єкт цілеспрямованої державної діяльності об'єднує всі компоненти, пов'язані з розвитком інформаційного суспільства, а саме: вільний доступ до інформації; інформаційну рівність, розвиненість та доступність інформаційних ресурсів; орієнтованість на національний інформаційний продукт; захищеність інформаційної інфраструктури тощо. Це означає, що перед державою, незважаючи на самоорганізаційні тенденції розвитку інформаційного суспільства, постає комплекс завдань, що передбачає як концептуальне стратегічне планування подальшого розвитку глобального інформаційного суспільства, так і створення механізмів безпосереднього захисту інформаційної інфраструктури окремих організацій, підприємств, установ, а також надання всебічної допомоги кожній людині з метою забезпечення реалізації права на інформацію.

РОЗДІЛ 3

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Правові властивості інформаційної безпеки

Декларування правової моделі розбудови сучасної української держави й поступове просування на цьому шляху зумовлюють домінування правових засад здійснення державної діяльності. Забезпечення інформаційної безпеки як один із найважливіших її напрямів не є винятком, що надає особливої актуальності правовим формам захисту і протидії негативним інформаційним впливам, ефективність яких прямо залежить від якості нормативно-правового забезпечення.

Сьогодні незадовільність стану українського інформаційного законодавства й необхідність термінових заходів із його удосконалення очевидні. Однак єдиної думки щодо шляхів якісної трансформації інформаційного законодавства України дослідники цієї проблематики не мають, що логічно, зважаючи на складність, динаміку та масштабність сучасних інформаційних процесів, які відбуваються в умовах становлення національної правової системи. Не можна не погодитися з твердженням В. П. Горбуліна та М. М. Биченка про те, що однією з основних причин невідповідності інформаційного законодавства України вимогам сучасності є несформованість у суспільній і науковій думці цілісного уявлення про інформаційну безпеку з позиції права та юридичної науки. Тому системний підхід до формування права і нормотворчості є актуальним завданням, зумовленим відсутністю належної систематизації чинного інформаційного законодавства. За відсутності методологічних засад інформаційного нормотворення виникають труднощі об'єктивного й суб'єктивного характеру при формуванні системи нормативно-правового регулювання інформаційної безпеки [66, с. 89].

Важливим підґрунтям удосконалення інформаційного законодавства виступає формування адекватного сучасним умовам уявлення про інформаційну безпеку в усій повноті її аспектів, зокрема психологічного, технічного та правового, з урахуванням глобалізаційних тенденцій.

Правове відображення належного рівня інформаційної безпеки – це сукупність правових умов, що забезпечують оптимальне функціонування і розвиток суб'єктів в інформаційному середовищі, частиною якого по суті є право як інформація про міру їхньої поведінки. Таке твердження дозволяє говорити, по-перше, про «інформаційно-правову безпеку», асоціюючи її з режимом законності в інформаційній сфері; по-друге, про правову інформацію як особливий предмет інформаційних відносин, універсальний організаційний засіб, який є важливим інструментом державного забезпечення інформаційної безпеки і, водночас, об'єктом захисту [326].

Виходячи з феноменологічних аксіологічних особливостей права, будь-яка форма його буття повинна розглядатися як загальнолюдська цінність. Серед онтологічних форм права традиційно виділяють ідею права, норми права, правовідносини, правосвідомість, правову культуру, правопорядок тощо. Очевидно, що в умовах глибокої інформатизації суспільного життя, коли інформація сама по собі набуває пріоритетного значення, правову інформацію також доцільно сприймати як одну з форм буття права і, відповідно, як складову правової реальності [24]. Причому в сучасному суспільстві, яке має яскраво виражений інформаційний вектор подальшого розвитку, вона становить особливу соціальну цінність. У такій якості, в межах концепції правової держави, якісна правова інформація може позиціонуватися на рівні пріоритетів національних інтересів, а отже, зумовлювати об'єктно-предметну спрямованість діяльності із забезпечення національної, зокрема інформаційної, безпеки.

Феномен правової інформації сьогодні залишається недостатньо дослідженим правовою наукою. Проте саме інформа-

ційний компонент визначає ефективність права як універсального соціального регулятора, оскільки в нормативному аспекті право є інформацією щодо можливого, належного, забороненого у важливих сферах суспільних відносин.

Із філософської точки зору «інформація» розглядається як віддзеркалення об'єктів матеріального світу. Тому процеси виникнення, створення, обміну, сприйняття, усвідомлення правової інформації в усіх її формах є своєрідним інформаційним виміром дії права, а сама правова інформація виступає елементом механізму правового регулювання, певним чином охоплюючи такі основні його елементи як норми права, правові акти, юридичні факти тощо. Саме такий підхід до правової інформації вбачається прагматичним і гармонійно пов'язаним із традиційними положеннями загальної теорії права, оскільки він відображає властивості правової інформації як складової основи, що забезпечує безпосередню реалізацію регулятивної функції права.

Проте сучасна вітчизняна нормативно-правова інтерпретація правової інформації, яка має бути найбільш прагматичною та раціональною, не повною мірою відповідає таким уявленням, є значно ширшою за змістом, що створює певну нормативно-правову невизначеність.

Так, Закон України «Про інформацію» (ст. 17) в останній редакції практично необмежено трактує поняття «правова інформація», відносячи до неї будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо. Очевидно, що таке визначення за своїм змістом має радше філософський науковий характер, ніж нормативно-правовий. При цьому серед джерел правової інформації тим же законом виділяються Конституція України, інші законодавчі й підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових пи-

тань [250], що акцентує увагу саме на нормативно-правових джерелах і засобах надання публічності їх положенням (змісту).

Альтернативні трактування правової інформації найчастіше ґрунтуються на тому чи іншому напрямі розуміння поняття «інформація» [39], трансформуючи його крізь поняття «правова сфера», яке є достатньо широким і не має конкретизованого визначення, наприклад: «правова інформація – відомості про факти, події, предмети, осіб, явища у правовій сфері життя суспільства, що містяться як у нормах права, так і в інших джерелах, і використовується при вирішенні правових завдань» [345].

Таким чином, у широкому розумінні, що сформувалося на сьогодні, правова інформація вбирає в себе значний масив суспільно важливої інформації і є не стільки окремим видом, скільки специфічною якістю тієї інформації, яка відображає процеси організації суспільного життя у сферах, охоплених правовим регулюванням. Специфіка правової інформації полягає ще й у тому, що, незалежно від змісту, вона завжди має певну соціальну значущість, яку їй і надає така якість, як «правота» або «правність».

Підтвердженням зазначеного вище можуть бути авторські інтерпретації класифікації правової інформації [2; 83; 151; 288], результат компіляції яких за обсягом і змістом буде наближатися до загальної класифікації інформації, яка пропонується в галузевих і спеціальних правових дослідженнях [178].

Отже, в межах широкого підходу, з певним ступенем умовності правову інформацію можна класифікувати за багатьма ознаками, зокрема:

1. За характером походження:

– інформація історично-теоретичного характеру – вироблена гносеологією, онтологією, аксіологією, антропологією, герменевтикою права тощо;

– інформація галузевого та прикладного характеру – вироблена галузевими та прикладними правовими науками;

– інформація інструментального характеру – отримана в процесі правотворчості й реалізації права.

2. За суб’єктами надання інформації:

– офіційна – інформація, надана уповноваженими державними органами, посадовими особами та органами місцевого самоврядування;

– неофіційна – будь-яка інша правова інформація, що надається суб'єктами, які не мають державно-владних повноважень.

3. За функціональною спрямованістю в механізмі правового регулювання:

1) нормативно-правова – інформація, яка міститься в правових актах і змістом якої є безпосередньо правові норми, тобто загальнообов'язкові правила поведінки;

2) індивідуально-правова – інформація, яка міститься в індивідуально-правових (правозастосовних) актах, спрямована на реалізацію правових норм і змістом якої є права та обов'язки конкретних суб'єктів у конкретних юридичних ситуаціях;

3) нормативно-технічна – інформація, яка відображає нормативні вимоги, стандарти в певних галузях діяльності, закріплені відповідними правовими актами;

4) допоміжна – будь-яка інша інформація пояснювального, рекомендаційного, процесуального та іншого характеру, необхідна для вирішення правових завдань, зокрема:

– пояснювальна – інформація, яка міститься в дефініціях і тлумаченнях;

– криміналістична – інформація, яка використовується під час доведення факту злочину та ідентифікації особи чи групи осіб, що вчинили злочин;

– судово-експертна – інформація, яка отримується під час судових експертиз із метою доведення (або спростування) фактичних обставин справи;

– оперативно-розшукова – інформація, яка відображає процес і результати проведення оперативно-розшукових заходів;

– статистично-інформувальна – інформація з різних галузей діяльності, необхідна для забезпечення процесів реалізації державно-владних повноважень (наприклад, статистика та розрахунки для прийняття державного бюджету; інформація про

стан довкілля, рівень життя населення, стан законності й правопорядку тощо).

4. За рівнем правових джерел – інформація, що міститься в міжнародних актах та актах національного законодавства (законах, підзаконних актах або інших видах правових актів, що відповідають типу правової системи).

5. За формою зовнішнього закріплення – документована і недокументована інформація.

6. За способом подання – інформація у вигляді письмових документів, в усній або конклюдентній формі, а також у вигляді електронних комп'ютерних даних.

7. За режимом доступу – відкрита, публічна, конфіденційна, секретна інформація тощо.

8. За суб'єктами отримання або надання інформації – інформація, отримана (надана) органами державної влади (законодавчими, виконавчими, судовими, контрольно-наглядовими), суспільними організаціями, іншими суб'єктами.

9. За формами активності – інформація, що створюється суб'єктами, отримується на добровільній основі (самостійне надання інформації іншими суб'єктами), отримується за вимогою (обов'язкове надання інформації іншими суб'єктами).

Звичайно, наведена класифікація не є вичерпною, проте дозволяє охопити загальні риси правової інформації та виділити її вузьке прагматичне розуміння з-поміж інших аспектів, що становлять широкий підхід, серед яких: інформація важлива для правової системи; інформація, що має юридичне значення; інформація, яка є об'єктом правовідносин; інформація, важлива для вирішення правових завдань тощо.

У вузькому розумінні поняття «правова інформація» має відображати основне призначення права як універсального регулятора суспільних відносин, а саме: правова інформація – це соціально важлива інформація, яка відображає нормативні (загальнообов'язкові) або індивідуальні вимоги до поведінки (діяльності) суб'єктів, що відповідають інтересам суспільства та забезпечуються й охороняються державою.

Такий аспект підкреслює ще одну властивість, яка принципово відрізняє правову інформацію від усієї іншої – обов'язковість її надання державою та усвідомлення відповідними суб'єктами. Так, Конституцією України кожному гарантується право знати свої права і обов'язки (ст. 57) і покладається обов'язок неухильно додержуватися Конституції України та законів України (ст. 68).

Отже, правова інформація у вузькому розумінні виступає основним засобом правового регулятивного впливу, що висуває до неї низку специфічних вимог. По-перше, традиційні герменевтичні вимоги до мови закону, від виконання яких залежить ефективність сприйняття правової інформації суб'єктом, якому вона адресована. До основних із них належать: офіційність стилю подання інформації, гармонійне поєднання ясності й простоти з точністю і повнотою, лаконічність, формалізованість, експресивна нейтральність, єдність використання термінології [349, с. 18–35]. По-друге, жорсткі вимоги як до життєво важливої суспільної інформації: об'єктивність, своєчасність, доступність, безкоштовність, публічність.

Сучасний етап розвитку людства характеризується суттєвим зростанням інтенсивності та обсягів потоків інформації. Від швидкості і якості їх оброблення значною мірою залежить ефективність управлінських рішень. Збільшується значення методів управління з використанням чітких інформаційних технологій соціальними та економічними процесами, фінансовими і товарними потоками; аналізу й прогнозування розвитку внутрішніх та зовнішніх ринків [295, с. 54]. Правове регулювання не є винятком. Інформаційний розвиток приводить до ускладнення форм взаємодії суб'єктів та виникнення нових сфер суспільних відносин, які має охоплювати правовий вплив, що зумовлює динамічні зміни в правовій сфері і, відповідно, зростання обсягів та інтенсивності потоків правової інформації. Своєчасне отримання якісної правової інформації та адекватне її сприйняття є визначальною умовою ефективності правового регулювання, а отже, і високого рівня «інформаційно-правової» безпеки.

Продемонструвати основні особливості означених вище процесів дає змогу абстрактна модель взаємодії суб'єктів у сфері правового регулювання, яка відображає технологію сучасної правової комунікації.

Основними її елементами є: 1) суб'єкт, зобов'язаний надавати правову інформацію (суб'єкт, наділений державно-владними повноваженнями, умовно – «законодавець»); 2) суб'єкт, зобов'язаний отримувати й усвідомлювати правову інформацію (умовно – «людина»); 3) середовище передавання та оброблення інформації, яким можуть виступати сучасні інформаційно-телекомунікаційні системи.

В умовах розвитку права взаємодія суб'єктів є двосторонньою. Правова інформація державно-владного характеру, створена «законодавцем», надається «людині», яка усвідомлює її, формуючи власну правосвідомість і правову культуру (правовий нігілізм), та трансформує в правову поведінку (правомірну, неправомірну), тобто реалізує або не реалізує надані їй можливості (суб'єктивні права) та покладені на неї обов'язки (юридичні обов'язки), певним чином формуючи законність і правопорядок та створюючи інформацію щодо їх стану. Останню збирає «законодавець» із метою коригування формалізованих правових вимог і державно-владного впливу, що веде до вдосконалення правового регулювання і забезпечує його розвиток.

Очевидно, що ефективність правової взаємодії безпосередньо залежить від властивостей трьох названих елементів. Інтелектуальні якості, ціннісні установки, рівень правосвідомості, правової культури, професіоналізму законодавця зумовлюють ступінь відповідності правової інформації суспільним закономірностям і потребам, а також усім технічним вимогам, які до неї висуваються. Правова культура і правосвідомість громадян визначають здатність адекватного сприйняття правових вимог, що на індивідуальному рівні зумовлює можливості їх реалізації. Але залишається третій елемент – середовище передавання та оброблення інформації, яке в епоху високих інформаційних технологій може відіграти одну з визначальних ролей у процесі оптимізації взаємодії держави й суспільства, підвищуючи шви-

дкість і надійність отримання правової інформації та надаючи її у формі, більш придатній для сприйняття.

Вплив сучасних інформаційно-телекомунікаційних технологій на правову культуру та правосвідомість виражається в такому: вони стають основним засобом і джерелом надання інформації про право, правову діяльність; дозволяють формувати правові орієнтири й установки; зумовлюють ефективність практичної діяльності у правовій сфері.

З метою підвищення рівня правосвідомості та формування соціально активної правомірної поведінки необхідна виважена державна політика у сфері створення і використання інформаційно-правових ресурсів, наповнення їх справді актуальною, якісною правовою інформацією [192, с. 10].

Підтвердженням цього є створення численних державних і комерційних пошукових електронних інформаційно-правових систем, які надають тексти правових актів, а також іншу корисну супутню інформацію у вигляді, придатному до автоматизованого оброблення. Майбутнє розвитку таких систем убачається в інтелектуальних інтерактивних геоінформаційних технологіях, які створять нові специфічні форми систематизації правової інформації. Це дозволить надавати громадянам не лише тексти правових актів у вигляді електронних друкованих сторінок, а й виважені з правової точки зору раціональні моделі правомірної поведінки. Наприклад, на запит щодо відкриття приватного підприємства має сформуватися відповідь зі всією необхідною інформацією (з урахуванням адміністративно-територіального розташування): відповідні статті законів та підзаконних актів, що визначають порядок реалізації права на відкриття приватного підприємства; назви повноважних організацій (їх юридичні адреси, контактна інформація, часи прийому); зразки документів, реквізити оплати послуг, вимоги до суб'єктів підприємницької діяльності тощо.

Окремим здобутком сучасних інформаційних технологій можна вважати програму «Електронний уряд», яка в Україні орієнтована на взаємодію в таких формах: 1) інформування

(надання безпосередньо інформації про державні (адміністративні) послуги); 2) одностороння взаємодія (забезпечення можливості користувачу отримати електронну форму документа); 3) двостороння взаємодія (забезпечення можливості оброблення електронної форми документа, включаючи ідентифікацію); 4) проведення трансакцій (електронна реалізація можливостей прийняття рішень) [241].

Найбільш ефективні у світі програми побудови електронного уряду включають розвиток інформаційно-телекомунікаційної інфраструктури й технологій, людських ресурсів і засобів доступу користувачів до інформаційних ресурсів держави [195]. Це означає, що для України ефективний «Електронний уряд» поки що залишається неблизькою перспективою.

Таким чином, від якості відповідної правової інформації й процесів її обігу багато в чому залежить ефективність сучасного забезпечення інформаційної безпеки. З одного боку, правова інформація перебуває під безпосереднім впливом процесів інформаційного розвитку суспільства, а з іншого – визначає правові механізми його становлення, що робить її специфічним компонентом змісту державної діяльності із забезпечення інформаційної безпеки, який має певні прояви в меті, засобах, принципах і результатах цієї діяльності.

Щодо законності в інформаційній сфері як асоціативного орієнтиру «інформаційно-правової» безпеки необхідно підкреслити таке. Поняття «законність» має досить складний і дискусійний характер. У запропонованому контексті розгляду інформаційної безпеки законність повинна сприйматися, виходячи з філософсько-правового розуміння закону, яке дозволяє розглядати її як загальноправове явище незалежне від особливостей правових систем та напрямів праворозуміння, якому в сучасних правових дослідженнях часто надається назва «правність» або «правозаконність».

Н. М. Оніщенко, абстрагуючись від пов’язаних із типом праворозуміння розбіжностей у численних дефініціях, зазначає,

що законність розуміють як фундаментальну юридичну категорію, яка є критерієм правового життя суспільства і громадян [213, с. 134]. Законність – це «комплексне політико-правове явище, що відображає правовий характер організації суспільного життя, органічний зв'язок права і влади, права і держави» [33]. Законність також розуміють як специфічний режим суспільно-політичного життя, втілений у системі нормативних, політико-правових вимог (неухильного дотримання правових актів усіма суб'єктами, верховенства права, рівності всіх перед законом, належного й ефективного застосування права, послідовної боротьби з правопорушеннями) [5, с. 194]. Законність у юридичному розумінні – це правовий режим у державі, за якого діяльність усіх державних органів, юридичних і фізичних осіб здійснюється відповідно до вимог закону [348, с. 214].

Отже, саме законність (правність) є необхідним організаційно-ідеологічним фундаментом, на якому можливе досягнення таких високих цілей, як розвиток громадянського й інформаційного суспільства і розбудова правової держави. Законність в інформаційній сфері життя суспільства й держави активно сприятиме цим процесам та забезпечуватиме стабільний інформаційний розвиток суспільства, ефективну взаємодію держави і громадян та громадян між собою, що по суті є метою забезпечення інформаційної безпеки.

Реалізація режиму законності в державі базується на системі гарантій, дієвість яких покликана зробити законність реальною [101, с. 210]. Гарантії законності носять достатньо широкий комплексний характер і мають як юридичну, так і загальносоціальну природу.

До загальносоціальних гарантій законності в інформаційній сфері належить уся сукупність умов існування суспільства (економічних, політичних, соціальних, ідеологічних тощо), які позитивно впливають на формування суспільної свідомості, зокрема її інформаційної складової.

У сучасній Україні ці умови знаходяться в зародковому стані, що гальмує загальний розвиток суспільства і створює пе-

репони на шляху реалізації законності та досягнення правопорядку. Тому практичне значення має аналіз загальносоціальних факторів як позитивного, так і негативного характеру, які є реальними умовами здійснення правового регулювання, становлення громадянського й інформаційного суспільства, розбудови правової держави, забезпечення національної та інформаційної безпеки з метою вироблення ефективних моделей державного управління та адекватних форм і методів здійснення державної влади.

Загалом сучасний етап розвитку української держави характеризується значною кількістю проблем у багатьох сферах суспільного життя. Задекларована на конституційному рівні модель України як незалежної, соціальної, демократичної, правової держави, незважаючи на окремі позитивні зрушення, залишається перспективою. Аналізуючи шляхи розбудови правової держави і громадянського суспільства в Україні, А. М. Колодій зазначає, що навіть загального погляду на нинішню соціально-економічну ситуацію достатньо, щоб переконатись у відсутності в ній ознак соціального громадянського суспільства. В сучасній Україні немає послідовної та виваженої державної програми (концепції) соціального розвитку, соціальної політики, довгострокової та незалежної від будь-якої влади, політичних сил, що нею володіють [134]. Ця думка свідчить про можливість дискусії щодо синергетичного характеру розвитку українського суспільства лише на теоретичному рівні, оскільки загальний рівень свідомості та самоорганізаційних можливостей індивідів ще дуже низький.

Отже, сьогодення України можна назвати початковим етапом становлення національної свідомості та зародження національної інформаційної свідомості, що надає особливого значення відповідному наявним умовам правовому регулюванню сфери інформаційних відносин.

Одним із головних завдань держави на цьому етапі розвитку є визначення напрямів правового регулювання і створення правових гарантій, необхідних для самореалізації суб’єктів в

інформаційній сфері. Виконання цього завдання ускладнюється низкою об'єктивних факторів, які виступають передумовами становлення інформаційного права України. Більшість із цих факторів є загальними чинниками (джерелами) процесу утворення національного права і тому дозволяють розглядати процеси розвитку інформаційного права України в контексті проблем становлення правової системи України загалом [321].

1. *Інтелектуальний (психологічний) фактор*. Сюди можна віднести ті характеристики української суспільної свідомості та явища негативного характеру, що в сукупності гальмують процеси інформаційного розвитку суспільства і забезпечення інформаційної безпеки:

– ірраціональність, консерватизм, апатичність суспільної свідомості;

– відсутність сформованості в загальносуспільній свідомості інформаційних потреб, зокрема у правовій інформації;

– відсутність усвідомленості інформаційних загроз;

– низький рівень правосвідомості громадян;

– падіння рівня загальної освіти й культури громадян;

– поширеність правового нігілізму.

2. *Варіативність та динамічність інформаційної сфери*. Ускладнює процеси утворення інформаційного права на всіх його етапах – формування, формулювання, реалізації. Цей фактор, маючи об'єктивний характер, призводить до недосконалості законодавства, що регламентує інформаційну сферу суспільних відносин, та неефективності його реалізації. Основними чинниками динамічності перетворень в інформаційній сфері є:

– стрімкий розвиток галузей діяльності людини, залежних від інформації;

– прогрес у інформаційно-комунікаційних технологіях;

– складність і різноманітність суспільних відносин в інформаційній сфері;

– новизна інформаційних відносин та відсутність досвіду їх правового регулювання;

– відсутність вироблених суспільством загальноприйнятих варіантів поведінки в інформаційній сфері.

3. *Підвищення соціального значення інформаційних процесів*. Визначає пріоритетність організаційно-забезпечувальної діяльності держави в інформаційній сфері як основи подальшого розвитку суспільства, що зумовлено такими чинниками:

– набуттям інформацією якостей життєво важливого ресурсу;

– всепроникністю інформаційних процесів;

– створенням широких інформаційно-комунікативних можливостей;

– виникненням додаткових можливостей саморозвитку суб'єктів;

– виникненням нових особливо небезпечних загроз суспільній безпеці;

– безпрецедентним підвищенням загальносоціального значення всіх складових інформаційної безпеки.

4. *Економічний фактор*. Створює економічне підґрунтя інформаційного розвитку суспільства й держави та матеріально-технічні можливості впровадження інформаційно-комунікаційних технологій. Узагальнені чинники економічного характеру, що визначають результативність процесу забезпечення інформаційної безпеки, такі:

– відсутність стабільного зростання економіки;

– низький рівень забезпеченості широких верств населення всіма необхідними для розвитку матеріально-технічними засобами;

– неналежне забезпечення апарату держави сучасними інформаційно-комунікаційними засобами;

– недостатність фінансування сфери освіти та науки.

5. *Техніко-технологічний фактор*. Його складові характеризують технічну досконалість та сучасність засобів обробления інформації, що визначає рівень технічної готовності до розгортання інформаційних процесів, а саме:

– нерозвиненість мережі швидкісного Інтернету;

– недосконалість інформаційних ресурсів;

– застарілість автоматизованих систем оброблення і захисту інформації.

6. *Політико-ідеологічний фактор*. Визначає рівень усвідомленості соціально сильними групами індивідів необхідності вирішення суспільних проблем в інформаційній сфері. Сюди можна віднести:

– відсутність сталої, не залежної від політичних персон, стратегії становлення України на світовій арені;

– відсутність реальної, послідовної та виваженої державної програми соціального розвитку;

– неправовий характер реалізації державної влади;

– переважання політичної доцільності над правовою;

– бюрократичність апарату держави;

– нерозвиненість громадянського суспільства;

– нерозвиненість інформаційних зв'язків між державою й суспільством;

– політизація засобів масової інформації;

– використання методик маніпулювання суспільною свідомістю під час політичної боротьби тощо.

Названі фактори наразі зумовлюють особливу важливість комплексної високопрофесійної державно-владної діяльності в інформаційній сфері, її правового забезпечення, а також виваженого вибору методів правового регулювання.

Юридичною основою створення сприятливих правових умов в інформаційній сфері можна вважати систему спеціально-юридичних та організаційних гарантій законності, яка складається із сукупності закріплених законодавством засобів та організаційно-правової діяльності із їх застосування, спрямованих на забезпечення інформаційної безпеки, а також заходів організаційного характеру, що забезпечують підвищення рівня інформаційної безпеки, боротьбу з правопорушеннями в інформаційній сфері, захист прав суб'єктів інформаційних відносин тощо.

Запропонована правова інтерпретація інформаційної безпеки надає їй певної системності (поєднання під правовим кутом зору економічних, ідеологічних, спеціально-юридичних,

організаційних важелів), що об'єктивно зумовлено міждисциплінарним характером інформаційної безпеки і правовим характером діяльності сучасної держави. Підтвердженням цієї позиції є популяризація останнім часом сучасними українськими спеціалістами з проблем національної безпеки виключно комплексного вирішення проблем інформаційної безпеки України. Так, В. П. Горбулін, М. М. Биченок, П. М. Копка серед актуальних проблем системного забезпечення інформаційної безпеки України виділяють такі напрями: нормативно-правове забезпечення, фінансово-економічні важелі, адміністративно-організаційні заходи, морально-етичне виховання та науково-технічне забезпечення [65, с. 79–86].

Комплексність підходу до забезпечення інформаційної безпеки зумовлює й необхідність широкого погляду на спеціально-юридичні гарантії законності в інформаційній сфері. Їх основою є наявність дієвого, ефективного, виваженого інформаційного законодавства, яке, що особливо актуально для України, відображатиме її інтеграційне спрямування та об'єктивні умови існування.

Сучасне трактування ефективності законодавства пов'язують із середовищем дії права, під яким розуміють взаємодію багатьох складових – стану економіки, політичного режиму, якості законодавства, ефективності роботи правових установ. Якщо ці чинники плідно взаємодіють, то формується певне правове середовище, що визначає правомірність дій суспільства, держави й індивіда [213, с. 86]. Проте в загальному вигляді потенційну ефективність і дієвість інформаційного законодавства України можна виразити за допомогою низки вимог, які визначають і проблематику наукових досліджень правового характеру у сфері забезпечення інформаційної безпеки:

– забезпеченість на рівні концепцій, принципів, дефініцій, які відображають багатоаспектність інформаційної безпеки;

– високий рівень законодавчої техніки та термінологічний комплекс, що відповідає всім вимогам до мови закону і юридичної термінології;

– адекватне відображення в інформаційному законодавстві реальних умов життя, напрямів розвитку суспільства, балансу інтересів держави, суспільства й особи, міжнародних стандартів;

– зручність інформаційного законодавства;

– передбачуваність ефективних механізмів реалізації;

– розвиненість і виваженість інституту юридичної відповідальності за правопорушення в інформаційній сфері.

Отже, у правовому вимірі інформаційна безпека певним чином інтегрується в явища правової реальності, які є традиційними об'єктами правової науки: законність і правопорядок, правосвідомість, норми права, правотворчість тощо. Це дозволяє стверджувати, що інформаційна безпека – не стільки нове явище для правової сфери, скільки чинник, який зумовлює певні її трансформації, а правові проблеми забезпечення інформаційної безпеки у своїй основі зумовлені проблемами розвитку правової системи, хоча і мають притаманні лише їм властивості.

Ефективність державної діяльності як із забезпечення інформаційної безпеки, так і в усіх інших сферах, значною мірою залежить від якості правового забезпечення. Правове забезпечення в нормативному розумінні є особливим видом інформації, зміст якої відбиває такі загальнолюдські цінності, як свобода, справедливість, формальна рівність, що висуває особливі вимоги до якості такої інформації й процесів її обігу. Дотримання цих вимог – один з основних шляхів підвищення ефективності правового регулювання в усіх сферах державного й суспільного життя, зокрема в інформаційній.

3.2. Міжнародні правові стандарти забезпечення інформаційної безпеки

Сучасні наукові дослідження інформаційної сфери, здійснені на пострадянському просторі, сформували достатньо широке розуміння інформаційної безпеки. Вона вже не асоціюється виключно з безпекою або захистом інформації. Інші не менш

важливі аспекти інформаційної безпеки розглядаються як її невід'ємні складові. Сьогодні серед них чітко виокремлюються інформаційно-психологічна безпека та інформаційна безпека у сфері прав і свобод людини, які закладають основи задоволення інформаційних потреб людини, її самореалізації та інформаційного розвитку суспільства загалом.

Європейською спільнотою безпосередньо інформаційній безпеці надається більш вузький зміст, який відображає переважно інформаційно-технічний аспект, хоча розвиток інформаційного суспільства визнається одним із пріоритетів. Аналогічні підходи властиві й іншим провідним країнам світу, зокрема США, Канаді, Японії. Передусім така ситуація пов'язана з усвідомленням і визнанням інформації як цінного ресурсу, а інформаційного розвитку – як сучасних засад підтримання конкурентоспроможності на міжнародній арені.

Поступово все більша частина людства долучається до реалізації програм становлення інформаційного суспільства, концепцій переходу до інформаційної доби, планів участі в трансформації суспільних інститутів тощо, прийнятих міжнародними організаціями ООН/ЮНЕСКО, Світовим банком, Світовою організацією торгівлі, Організацією економічного співробітництва і розвитку, Радою Європи, Європейським Союзом, Європейським банком реконструкції і розвитку та іншими міжнародними й регіональними урядовими і неурядовими інституціями, які, зокрема, можуть розглядатися як суб'єкти забезпечення інформаційної безпеки. Основною метою цих документів є визначення стратегічних напрямів розвитку інформаційного суспільства, основних положень, умов і пріоритетів міжнародної, регіональної та національної інформаційної політики, а також політичних, правових, соціально-економічних, культурних та технологічних передумов переходу до інформаційного суспільства [173, с. 42].

Забезпечення інформаційної безпеки в широкому розумінні має нерозривний сутнісний зв'язок із розвитком інформаційного суспільства як на теоретичному, так і на практичному рівні. Виділення ж таких змістових елементів забезпечення інфор-

маційної безпеки, як: мета – суспільство, в якому забезпечується вільний доступ, створення та обмін інформацією, а також інтеграція у світовий інформаційний простір; об'єкт – людина і її права на інформацію; суб'єкти – міжнародні організації; засоби та методи – правове регулювання; принципи – гарантованості доступності інформації, інформаційної рівності, використання в інтересах країни міждержавних систем та механізмів міжнародної колективної безпеки – зумовлює особливу важливість приєднання до міждержавних програм розвитку інформаційного суспільства.

Еру становлення глобального інформаційного суспільства започаткувала Окінавська хартія глобального інформаційного суспільства, ухвалена 22 липня 2000 року лідерами країн "великої вісімки".

У вступній частині Хартії зазначається, що інформаційно-телекомунікаційні технології є одним із найбільш важливих факторів, що впливають на формування суспільства двадцять першого сторіччя, створюючи величезні додаткові можливості в житті людей, їх освіті й роботі, а також взаємодії уряду і громадянського суспільства.

Окремо визначається, що сутність стимульованих інформаційно-телекомунікаційними технологіями економічних та соціальних трансформацій полягає в їх здатності сприяти людям і суспільству у використанні знань та ідей із метою розвитку свого потенціалу та реалізації своїх прагнень. При цьому визнаються необхідними гарантії забезпечення сталого економічного зростання, підвищення суспільного добробуту і створення соціальної злагоди, а також реалізації потенціалу інформаційно-телекомунікаційних технологій у сфері зміцнення демократії, більш прозорого та відповідального управління, в захисті прав людини й сприянні збереженню культурного розмаїття, збереженні миру та стабільності у всьому світі [207].

Стрижневою основою Хартії є визнання необхідності подолання електронно-цифрового розриву всередині держав та між ними, оскільки саме цей фактор гальмує формування гло-

бального інформаційного суспільства й забезпечення реальної інформаційної рівноправності. З цією метою, підкреслюючи важливу роль приватного (недержавного) сектору, країни-учасники декларують тверді наміри щодо:

– сприяння політичному діалогу між партнерами і зацікавленості світової спільноти щодо сучасних викликів та можливостей;

– сприяння використанню інформаційно-комунікаційних технологій у соціальній сфері (подолання бідності, освіта, культура, охорона здоров'я);

– розвитку людського потенціалу шляхом розширення можливостей як базової, так і спеціальної освіти у сфері інформаційно-комунікаційних технологій, а також в інших актуальних галузях, зокрема правовій;

– стимулювання інформаційно-змістовної національної продукції;

– підтримання країн, які розвиваються, шляхом обміну досвідом, консультування, підготовки фахівців, а також пошуку оптимальних шляхів забезпечення технічної сумісності;

– стимулювання розроблення інноваційних підходів до здешевлення доступу до глобальних мереж;

– заохочення підприємців до участі в процесах інформаційного розвитку, зокрема, стимулювання електронної торгівлі тощо.

Хоча в Хартії безпосередньо не йдеться про необхідність забезпечення інформаційної безпеки, але практично в кожному пункті наголошується на важливих проблемах, які визначають напрями забезпечення інформаційної безпеки глобального інформаційного суспільства, а саме:

– захист прав людини й сприяння збереженню культурного розмаїття;

– сприяння формуванню мережевої культури та довіри;

– забезпечення рівного, вільного та безпечного доступу всіх до інформаційних ресурсів (подолання електронно-цифрового розриву);

– створення передбачуваної, прозорої й недискримінаційної інформаційної політики та нормативної бази;

– протидія зловживанням, що підривають цілісність інформаційної мережі;

– боротьба з кіберзлочинністю (зокрема хакерством і розповсюдженням комп'ютерних вірусів) та протидія транснаціональній організованій злочинності;

– захист інтелектуальної власності;

– удосконалення механізмів захисту конфіденційності, а також захисту оброблення персональних даних за умов збереження вільного інформаційного потоку;

– розвиток людських ресурсів (подолання комп'ютерної неграмотності; загальна освіта, професійна підготовка в інформаційній сфері) [207].

Таким чином, Окінавська хартія є закликом міжнародної спільноти як на державному, так і на приватному рівні до ліквідації розриву в рівні використання інформації і знань, до консолідації зусиль на шляху побудови глобального інформаційного суспільства та забезпечення його безпечного існування, що сприятиме вирішенню економічних і соціальних світових проблем та утверджуватиме у світі демократичні цінності.

Однак Окінавські домовленості 2000 року не були безпрецедентними у свій час. Одним із перших здобутків міжнародної співпраці, що відіграв важливу роль у формуванні уявлень щодо можливої стратегії розбудови інформаційного суспільства в глобальному масштабі, стала прийнята на 29-й сесії Генеральної Конференції ЮНЕСКО в 1996 році концепція «Інформаційне суспільство для всіх» [353], яка знайшла своє продовження в низці програм під егідою ООН/ЮНЕСКО, відомих під назвами «На шляху до комунікаційного та інформаційного суспільства», «Комунікація, інформація, інформатика», «Інформація для всіх» та інших.

Виходячи з положень ст. 19 Загальної декларації прав людини, яка закріплює свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від держа-

вних кордонів [100], цими програмами ЮНЕСКО відводить собі провідну роль у формуванні глобального інформаційного суспільства, в якому інформація сприймається передусім як знання та забезпечується вільний доступ усіх до неї.

Як підкреслив напередодні Женевського саміту з питань інформаційного суспільства 2003 року Генеральний директор ЮНЕСКО Коіто Мацуура, з точки зору ЮНЕСКО розвиток інформаційного суспільства повинен привести до створення «суспільств знань», тому немає сенсу говорити про інформаційне суспільство і, тим більше, про суспільство знань, якщо не забезпечити вільний і безкоштовний доступ до інформації та знань у всіх їх формах і на всіх носіях [58].

Визнаючи провідну роль інформації в процесах розвитку людства та виступаючи каталізатором діяльності держав, ЮНЕСКО пріоритетною метою на межі 2000 року визначила створення платформи для дискусії щодо міжнародної політики у сфері захисту інформації і всезагального доступу до неї, стосовно всезагальної участі в глобальному інформаційному суспільстві, а також щодо моральних, правових та суспільних наслідків розвитку інформаційно-телекомунікаційних технологій.

Серед напрямів своєї роботи ЮНЕСКО називала:

– заохочення й розширення доступу до інформації за допомогою її організації, перетворення на цифрову електронну форму й захисту;

– розвиток міжнародної рефлексії та дискусій щодо етичних, правових і суспільних загроз та викликів в інформаційному суспільстві;

– сприяння тренінгу, безперервній освіті й навчанню у сфері інформації та інформатики;

– просування використання міжнародних стандартів і передового досвіду у сфері інформації та інформатики в межах компетенції ЮНЕСКО;

– просування мережевої взаємодії у сфері інформації й знань на локальному, національному, регіональному та міжнародному рівнях [258].

На сьогодні діяльність ЮНЕСКО щодо розвитку інформаційного суспільства має більш практичне окреслення. Так, Стратегічним планом програми «Інформація для всіх» на 2008–2013 роки сформульовано всеосяжну мету програми – «надання країнам-членам допомоги в розробленні і здійсненні національної інформаційної політики й стратегій з обміну знаннями в умовах зростання ролі цифрових технологій». Цим же документом визначено п'ять конкретизованих пріоритетів: «Інформація з метою розвитку», «Інформаційна грамотність», «Збереження інформації», «Інформаційна етика», «Доступність інформації» [294].

Серед основних негативних чинників, що гальмують розбудову глобального інформаційного суспільства, в документах ЮНЕСКО логічно виокремлюються:

– інформаційно-технологічний дисбаланс та інформаційна ізоляція окремих регіонів і країн (збільшення розриву між інформаційно багатими та інформаційно бідними країнами);

– негативні впливи (наслідки розвитку) інформаційно-телекомунікаційних технологій;

– загрози інформаційним правам і свободам людини (громадянина), включаючи право на доступ до інформації й конфіденційність інформації, а також розповсюдження інформації расистського, агресивного та дискримінаційного характеру; інформаційна неосвіченість і різниця у володінні інформаційними навичками [174, с. 80].

Загальний аналіз програм ЮНЕСКО дозволяє виділити дві основні складові її діяльності в напрямі розвитку інформаційного суспільства й забезпечення інформаційної безпеки:

1) сприяння вільному поширенню інформації (ідей, знань) і загальному доступу до неї;

2) збагачення комунікаційного та інформаційного потенціалу з метою забезпечення всім націям і спільнотам можливості брати участь у світових процесах розбудови глобального інформаційного суспільства.

Єдиний ідеологічний напрям з Окінавською хартією та програмами ЮНЕСКО мають міжнародні домовленості, досяг-

нуті на Всесвітніх зустрічах на вищому рівні з питань інформаційного суспільства, які відбулися в Женеві (2003 рік) та Тунісі (2005 рік), проведених Організацією Об'єднаних Націй і Міжнародним союзом електрозв'язку.

За підсумками Женевської зустрічі 2003 року було прийнято Декларацію принципів, яка сформувала бачення концепції становлення інформаційного суспільства як «глобального завдання в новому тисячолітті» [54].

Декларацією учасники зустрічі висловили «спільне прагнення та рішучість у побудові орієнтованого на інтереси людей, відкритого для всіх і спрямованого на розвиток інформаційного суспільства, в якому кожен міг би створювати інформацію і знання, мати до них доступ, користуватись і обмінюватись ними, з метою надання окремим особам, общинам і народам можливостей повною мірою реалізувати свій потенціал, сприяючи своєму стабільному розвитку та підвищуючи якість свого життя на основі цілей і принципів Статуту ООН і дотримуючись в повному обсязі та підтримуючи Загальну декларацію прав людини» [54].

Окремими пунктами Декларації наголошується на центральній ролі науки в розвитку інформаційного суспільства, оскільки «більшість компонентів інформаційного суспільства» є результатом спільних науково-технічних досягнень, а також на усвідомленні, що за сприятливих обставин інформаційно-комунікаційні технології стають «потужним інструментом» підвищення якості життя людей. При цьому акцентується увага на нерівномірному розподілі переваг, які надають інформаційні технології, між розвиненими країнами та країнами, що розриваються, а також між окремими верствами населення, серед яких діти, жінки, біженці, безробітні й люди з обмеженими можливостями. Тобто наявний «цифровий розрив», як і Окінавською хартією, визнається центральною проблемою на шляху становлення інформаційного суспільства.

Таким чином, Декларацією принципів інформаційне суспільство визнається не самоціллю, а новою суспільною форма-

цією, покликаною утверджувати визнані загальнолюдські цінності й покращувати життя всіх людей. При цьому інформація виступає засобом розвитку людини, ресурсом знань, до якого кожен повинен мати доступ.

Загальна концепція інформаційного суспільства і керівні положення Декларації принципів знайшли своє втілення в Плані дій, також прийнятому на Женевському саміті 2003 року [55].

План дій має більш конкретизований зміст і визначає основні напрями діяльності, які ведуть до досягнення цілей розвитку, узгоджених на міжнародному рівні, шляхом сприяння широкому впровадженню інформаційно-комунікаційних технологій, а також спрямовані на подолання розриву в цифрових технологіях.

Третім пунктом Плану окреслюється роль органів державного управління, міжнародних і регіональних установ, інститутів громадянського суспільства та приватного сектору в становленні інформаційного суспільства. Відзначаючи безперечну важливість діяльності кожної з названих інституцій та злагодженості їх спільних дій у всіх напрямах, провідну роль у формуванні національних стратегій інформаційного розвитку План відводить державі. Разом із тим, участь приватного сектору має велике значення для активізації процесів інформатизації, міжнародні організації відіграють ключову роль в інтеграційних процесах, а громадянське суспільство покликане сприяти збереженню та примноженню загальнолюдських цінностей, передусім справедливості.

Серед спільних напрямів діяльності згідно з Планом дій логічно виокремлюються:

1) розвиток інформаційно-комунікаційної інфраструктури на основі новітніх технологій;

2) популяризація електронних інформаційних ресурсів та забезпечення всезагального доступу до них;

3) сприяння освіті у сфері інформаційно-комунікаційних технологій та інформатизація освіти загалом;

4) створення сприятливих політичних, економічних, правових умов для розвитку інформаційно-комунікаційних техно-

логій, зокрема Інтернету як важливого засобу розвитку інформаційного суспільства;

5) забезпечення безпеки й надійності використання інформаційно-комунікаційних технологій;

6) глибока інформатизація суспільно важливої діяльності – державного управління, комерції, науки, навчання, охорони здоров'я, охорони навколишнього середовища, сільського господарства, а також сфери культури й засобів масової інформації;

7) утвердження загальнолюдських цінностей (свобода, справедливість, рівність, толерантність, відповідальність, збереження природних ресурсів);

8) міжнародне та регіональне співробітництво з метою подолання цифрового розриву.

На відміну від інших розглянутих міжнародних документів, План дій певною мірою конкретизує і сферу забезпечення інформаційної безпеки. Так, його пунктом 12 довіра й безпека відносяться до «головних опор інформаційного суспільства». Цей же пункт містить прямі настанови органам державного управління, за підтримки приватного сектору, щодо попередження і виявлення проявів кіберзлочинності та неналежного використання інформаційно-комунікаційних технологій шляхом застосування необхідних заходів правового й організаційного характеру, міжнародної співпраці та сприяння обізнаності людей щодо нових загроз конфіденційності їх життя й способів захисту від них.

Привертає увагу й логічне надання прагматичності підходам до практичної оцінки стану розвитку інформаційного суспільства, що в сутності є і відображенням стану інформаційної безпеки. Для цього пунктом 28 установлюється загальне завдання щодо розроблення і впровадження реалістичної міжнародної системи якісних і кількісних оцінок рівня розвитку інформаційного суспільства.

Наступний саміт із питань інформаційного суспільства, проведений у Тунісі у 2005 році, підтвердив усі попередні прагнення та цілі щодо розвитку інформаційного суспільства. Його

результатами стало прийняття Туніського зобов'язання і Туніської програми для інформаційного суспільства [56; 57].

Туніське зобов'язання стало черговим закликом світової спільноти до консолідації зусиль на шляху розбудови відкритого для всіх, справедливого інформаційного суспільства. При цьому відмічено основоположну роль інформаційно-комунікаційних технологій для економічного зростання, необхідність усунення перешкод на шляху подолання «цифрового розриву», а також необхідність ефективної протидії проблемам і загрозам, що виникають унаслідок використання інформаційно-комунікаційних технологій усупереч цілям підтримання міжнародної безпеки й стабільності. Серед таких загроз зазначається зловживання інформаційними ресурсами і технологіями зі злочинними й терористичними цілями та недотримання прав людини [56].

Особливістю Туніської програми для інформаційного суспільства є те, що поряд із напрямами вирішення фінансових питань щодо подолання «цифрового розриву» широко піднімаються проблеми Інтернету, який визнається цим документом основним елементом інфраструктури інформаційного суспільства, що перетворився з науково-дослідного й навчального інструменту на загальнодоступний глобальний інструмент. У зв'язку з цим гостро ставляться питання глобальної безпеки Інтернету, а саме: постійний розвиток культури кібербезпеки, посилення захисту інформації особистого характеру і персональних даних, удосконалення механізмів притягнення до кримінальної відповідальності за кіберзлочини (включаючи злочини, скоєні в межах юрисдикції однієї країни, які призвели до наслідків в іншій країні), а також вирішення проблем із поширенням спаму [57].

Розглянуті міжнародні акти свідчать, що країни – члени ООН намагаються докладати значних зусиль для досягнення світової злагоди і забезпечення належного рівня життя шляхом розбудови глобального інформаційного суспільства. Водночас за результатами Оцінки прогресу, досягнутого в здійсненні рі-

шень, і подальшої діяльності за підсумками Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства, представленої Економічною та Соціальною Радою ООН у 2010 році, поряд із позитивними здобутками відмічаються недостатні темпи скорочення цифрового розриву, особливо щодо можливостей користування швидкісним інтернетом, що призводить до посилення нерівності доступу до інформаційно-телекомунікаційної інфраструктури між розвинутими країнами і країнами, що розвиваються, а також різними верствами населення [220].

Давню правову історію має суто європейський досвід становлення інформаційного суспільства. Серед перших нормативно-правових актів, спрямованих на вирішення питання становлення інформаційного суспільства в ЄС, – Резолюція Європейського Союзу «Біла Книга. Зростання, конкурентоспроможність, зайнятість: виклики та стратегії XXI століття» 1993 року, Директива ЄС «Зелена Книга. Життя і працевлаштування в інформаційному суспільстві» та Рекомендація «Інформаційна магістраль для глобального суспільства» 1996 року [360; 363; 365].

Діалектичний взаємозв'язок європейської і глобальної стратегій становлення інформаційного суспільства представлено в концептуальній доповіді Європейської комісії з проблем інформаційного суспільства «Європа і глобальне інформаційне суспільство: рекомендації для Європейської Ради ЄС» 1994 року. У ній зазначається, що глобальні інформаційні процеси впливають на становлення нової ієрархії держав, відкривають нові можливості промислового розвитку, зумовлюють створення відповідної правової бази, підвищують рівень обміну культурою та традиціями [174, с. 85]. «Європа усвідомлює важливість глобального співробітництва і необхідність правил для інформаційного суспільства, які стосуються права на інтелектуальну власність, недоторканність приватного життя, охорони персональних даних, інформаційної безпеки, використання інформаційного ресурсу, заборони незаконної інформації. В документах підкреслюється, якщо Європа не зможе ефективно адаптуватися до нових умов, вона втратить конкурентоспромож-

ність на світових і регіональних ринках і матиме соціальні проблеми в європейських країнах» [355; 359].

Квінтесенцією цієї доповіді є визначення становища держави в міжнародному середовищі не за географічним розташуванням, кількістю природних ресурсів, кліматичними умовами та соціально-економічним потенціалом, а за рівнем упровадження наукових досягнень і високих технологій в усі сфери життєдіяльності суспільства.

Реалізація стратегії інформаційного суспільства в Європейському Союзі ґрунтується на потужному матеріально-фінансовому забезпеченні. Для розвитку ідей інформаційної політики Європейського Союзу в окремих сферах життєдіяльності суспільства створюються програми та проекти, а саме: «Розвиток технологічних досліджень», «Інформаційні технології і ринкова політика», «Європейська стратегічна програма промислового розвитку і впровадження технологій», «Он-лайн для урядів», «Глобальна інвентаризація», «Електронна комерція», «Дистанційна освіта, медицина, культура та інформаційні послуги» [174, с. 86].

Як орієнтир діяльності практичну цінність для України мають європейські програми, сформовані в межах Лісабонської стратегії (Lisbon Strategy) 2000 року [362]. Їх відображенням є послідовні плани дій становлення інформаційного суспільства і забезпечення безпеки головного стратегічного інструменту – мережі Інтернет. До них належать низка планів дій «Електронна Європа» («e-Europe») та «Безпечніший Інтернет» («Safer Internet»).

Загалом Плани дій «e-Europe» охоплюють багато напрямів, які згруповані навколо трьох основних пріоритетів:

1) дешевий, швидкий, безпечний інтернет;

2) інвестиції в людей та їхні інформаційно-комунікаційні навички;

3) стимулювання використання інтернету в різних галузях діяльності.

Для України, зокрема, достатньо актуальними сьогодні є пріоритети, які визначалися Планом дій «e-Europe 2005»:

– поширення і використання швидкісних мереж на всій території за конкурентними цінами;

– розвиток системи електронних послуг (електронний уряд, електронне навчання, електронна охорона здоров'я);

– підвищення динаміки електронної комерції;

– безпечна інформаційна інфраструктура [357; 358].

План дій «Safer Internet Plus 2005–2008» установлює не менш актуальні для українського електронного інформаційного простору напрями діяльності, основні з яких:

1) створення безпечного середовища за допомогою широкої мережі «гарячих ліній» екстреного зв'язку;

2) підвищення поінформованості людей щодо способів захисту від інформації, яка має шкідливий зміст;

3) боротьба з небажаним і шкідливим змістом шляхом використання технологічних досягнень;

4) сприяння охороні навколишнього середовища шляхом створення спеціальних інтернет-ресурсів [352].

Особливим здобутком європейської співпраці, що заслуговує окремої уваги, є Конвенція Ради Європи про кіберзлочинність 2001 року, яка здійснила прорив у забезпечення інформаційної безпеки, заклавши основи світових стандартів протидії злочинам у сфері інформаційно-комунікаційних технологій [138].

Виходячи із численних міжнародних домовленостей і рішень світового та європейського масштабу, спрямованих на забезпечення безпеки інформаційно-комунікаційних технологій та забезпечення прав людини під час їх використання, Конвенція покладає на держави, які її підписали, зобов'язання встановлення кримінальної відповідальності за поведінку, що вважається проявом кіберзлочинності: незаконний доступ до комп'ютерних систем; нелегальне перехоплення комп'ютерних даних, які не призначені для публічного користування; втручання в дані; втручання в систему; зловживання пристроями; підробка і шахрайство, пов'язані з комп'ютерами; правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських та суміжних прав.

Крім того, Конвенцією на загальному рівні врегульовуються питання надання повноважень, достатніх для ефективної боротьби з означеними кримінальними правопорушеннями «шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва» [138].

Підписання Конвенції про кіберзлочинність є важливим кроком міжнародної спільноти на шляху практичного забезпечення інформаційної безпеки в глобальному масштабі. Наявні й інші міжнародні досягнення в галузі безпосереднього забезпечення інформаційної безпеки на рівні окремих організацій (підприємств, установ, компаній тощо) різних форм власності. Найвідоміші з них – узагальнені принципи організації системи управління інформаційною безпекою, які отримали назву «Стандарти управління інформаційною безпекою» та завдяки своїй ефективності набули широкого визнання, ставши основою національних стандартів багатьох сучасних держав.

Першопричиною виникнення стандартів управління інформаційною безпекою були потреби великих комерційних структур у забезпечення власної інформаційної безпеки, особливо стосовно захисту комерційної таємниці та належного забезпечення доступу до інформаційних ресурсів. Однак комплексність підходів, закладена цими стандартами, є практичним втіленням багатьох концептуальних положень міжнародних актів щодо забезпечення інформаційної безпеки і, зокрема, ефективним превентивним заходом протидії кіберзлочинності.

Родоначальником низки сучасних міжнародних стандартів у галузі систем управління інформаційною безпекою (СУІБ) став стандарт BS 7799, розроблення якого Британським інститутом стандартів BSI (British Standards Institution) почалася ще 1995 року [112].

Положення цього стандарту на добровільній основі застосовує велика кількість компаній у десятках країн світу (у 27 країнах видано понад 1100 сертифікатів відповідності). Сертифікація системи управління інформаційною безпекою на відпо-

відність стандарту BS 7799 дозволяє власникам інформаційних ресурсів та їх партнерам переконатися в тому, що підсистема інформаційної безпеки побудована правильно й функціонує ефективно.

Слід зазначити, що стандарт BS 7799 не є технічним. Він, зокрема, не пропонує використання певних способів шифрування даних або засобів апаратного захисту, а лише визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, відповідальність співробітників, використання оцінки ризиків тощо в контексті забезпечення інформаційної безпеки.

До основних напрямів управління інформаційною безпекою стандарт BS 7799 включає:

– захист інформації від несанкціонованого доступу (захист конфіденційності інформації);

– захист інформації від несанкціонованої зміни, забезпечення її точності й повноти (захист цілісності інформації);

– забезпечення можливості користування інформацією (забезпечення доступності інформації).

Певної універсальності цьому стандарту надає й те, що він не концентрується лише на конфіденційності. У комерційних організаціях, із погляду можливих матеріальних втрат, цілісність і доступність даних найчастіше є більше критичними.

Серед можливих загроз, на протидію яким орієнтовано стандарт, виділяються:

– хакерські атаки;

– зараження комп'ютерними вірусами;

– комп'ютерне піратство;

– промислове шпигунство;

– фізичне втручання в комп'ютерні системи;

– несумлінність персоналу;

– надійність апаратно-програмних засобів тощо [354].

Таким чином, основну мету Стандарту можна сформулювати як створення загальної методології для розроблення, впровадження й оцінювання ефективності систем управління інформаційною безпекою, що може застосовуватись в умовах як ко-

мерційних компаній, так і державних та некомерційних структур із чисельністю в десятки тисяч співробітників.

На основі стандарту BS 7799 Міжнародною організацією стандартизації ISO (International Organization for Standardization) та Міжнародною електротехнічною комісією IEC (International Electrotechnical Commission) розроблено сімейство стандартів ISO/IEC 27000, які удосконалюються і доповнюються кожного року. Також проводиться його уніфікація з популярними стандартами управління COBIT (Control Objectives for Information and related Technology – Міжнародний стандарт управління інформаційними технологіями) й ITIL (Information Technology Infrastructure Library – бібліотека інфраструктури інформаційних технологій) та іншими.

Крім управління інформаційною безпекою, є ще один напрям стандартизації – захист інформації з обмеженим доступом, особливо важливий на державному рівні. До відомих стандартів у цій сфері належить розгалужена система стандартів STANAG (Standardization Agreement), більшість яких повторюють стандарти військового відомства США – MILStandart [364] і є основою політики захисту інформації з обмеженим доступом країн НАТО [284, с. 24]; а також канадський Стандарт CSA 1996 року, який Міжнародною організацією стандартизації було покладено в основу розвитку міжнародних стандартів щодо персональної інформації, зокрема ISO 29100 «Information technology. Security techniques. Privacy framework» (Інформаційні технології. Методи забезпечення безпеки. Межі конфіденційності) [47, с. 123].

Слід зазначити, що Україна не в авангарді широкого впровадження міжнародних стандартів у сфері забезпечення інформаційної безпеки, хоча необхідність цього процесу сьогодні вже усвідомлена. Так, Доктриною інформаційної безпеки України серед напрямів державної політики у сфері забезпечення інформаційної безпеки зазначається гармонізація вітчизняного законодавства з питань інформаційної безпеки в економічній сфері з міжнародними нормами і стандартами [247]. Крім того, ще у 2002 році Проект Концепції національної інформаційної полі-

тики як одну з основних вимог до національної інформаційної інфраструктури визначав відповідність міжнародним стандартам і рекомендаціям Міжнародного телекомунікаційного союзу (ITU), Європейської конференції адміністрацій поштового та електрозв'язку (CEPT) і Міжнародної організації стандартизації/Міжнародної електротехнічної комісії (ISO/IEC), що повинно сприяти взаємодії технічних засобів, інформаційних пристроїв і послуг із тими, що діють у світовому інформаційному просторі в складі Глобальної інформаційної інфраструктури [251].

Утім, упровадження стандартів управління інформаційною безпекою в Україні просувається вкрай повільно. Наразі офіційного визнання набули лише два, як галузеві стандарти банківської сфери, введені в дію Національним банком України: СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IES 27001:2005, MOD) та СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO/IES 27002:2005, MOD) [107; 253]. Прикладом для України в цьому напрямі може бути досвід Російської Федерації, яка впроваджує міжнародні стандарти управління інформаційною безпекою на рівні державних (національних) стандартів із 2005 року [68; 69].

Теоретично альтернативним для України на шляху становлення інформаційного суспільства й забезпечення інформаційної безпеки міг би стати досвід євразійської міжнародної співпраці, зокрема напрацьований Шанхайською організацією співробітництва (ШОС) і Євразійським економічним співтовариством (ЄврАзЕС). Проте проблеми становлення інформаційного суспільства не привертають увагу на рівні офіційних документів навіть як перспективні, а питання забезпечення інформаційної безпеки сприймаються більшою мірою в контексті спрямованості діяльності цих організацій.

Так, представниками ШОС у 2007 році, разом із підписанням Бішкекської декларації, був затверджений План дій із забезпечення міжнародної інформаційної безпеки, який стосується спільної протидії кіберзлочинності та кібертероризму, що

розглядається в рамках співробітництва в боротьбі з тероризмом, сепаратизмом і екстремізмом [217].

Із результатів діяльності ЄврАзЕС корисними досвідом для України можуть стати типові проекти законів, серед яких і проект закону «Про інформаційну безпеку», розроблені в межах створення Податкового союзу і Єдиного економічного простору [205]. Зауважимо, що ці типові проекти формують певні законодавчі стандарти для країн – членів ЄврАзЕС у сфері інформаційно-комунікаційних технологій.

Отже, загальний аналіз міжнародних актів, спрямованих на сприяння інформаційному розвитку, дозволяє зробити низку висновків.

По-перше, ціннісними орієнтирами, що визначають концепцію подальшого розвитку світового суспільства, є:

– інформаційне суспільство як пріоритетний шлях світового розвитку;

– інформація, що визнається цінним ресурсом і становить знання, необхідні для розвитку та добробуту людини;

– принцип рівності доступу до інформаційних ресурсів, свободи та справедливості, без втілення якого не можлива розбудова глобального інформаційного суспільства.

По-друге, основними завданнями на шляху становлення інформаційного суспільства визнаються:

– усунення інформаційної нерівності (цифрового розриву) як усередині країн, так і між ними;

– інформатизація життєво важливих галузей суспільної діяльності;

– забезпечення безпечного використання інформаційно-комунікаційних технологій, передусім, мережі Інтернет як основного інструменту розвитку інформаційного суспільства.

По-третє, найбагатшу правову історію розвитку інформаційного суспільства мають країни європейського регіону, які мають бути орієнтиром для України.

По-четверте, слід відзначити, що Україною вже зроблені суттєві кроки на шляху до повноправної участі у світових процесах становлення інформаційного суспільства. Найважливішими з них можна вважати ратифікацію Конвенції про

кіберзлочинність (2005 рік) та прийняття Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» (2007 рік), який відобразив українське концептуальне бачення інформаційного суспільства. Порівняльний аналіз цього закону з розглянутими положеннями міжнародних актів доводить, що Україна повністю поділяє ідеали інформаційного суспільства, сформовані світовою та європейською співпрацею.

Можна також погодитись із позицією Ю. Є. Максименко, яка зазначає, що «українські та європейські норми, що регулюють суспільні відносини забезпечення інформаційної безпеки у сфері прав та свобод, є більш узгодженими щодо інших аспектів інформаційної безпеки, відтак не становлять серйозної проблеми для адаптації» [174, с. 109].

Усе це дозволяє стверджувати, що, безперечно, орієнтирами для державної політики України в напрямі вирішення проблем забезпечення інформаційної безпеки мають бути: по-перше, продовження міжнародної, зокрема європейської, співпраці з інформаційно розвиненими державами, спрямованої на повноцінне приєднання до програм інформаційного розвитку та гармонійне впровадження отриманого досвіду в справу розбудови майбутнього українського суспільства; по-друге, продовження гармонізації положень міжнародних актів із законодавством України (особливо це стосується вимог Конвенції про кіберзлочинність); по-третє, посилення практичної реалізації задекларованих намірів щодо розвитку національної інформаційно-комунікаційної інфраструктури, створення якісних і доступних інформаційних ресурсів, інформатизації освіти й науки, підтримання національної інформаційної продукції, забезпечення повсюдного доступу всіх громадян до мережі Інтернет, розширення можливостей отримання електронних послуг, широке впровадження визнаних світових стандартів у сфері безпеки інформаційно-телекомунікаційних технологій тощо.

3.3. Інформаційне законодавство як гарантія забезпечення інформаційної безпеки в Україні

У правових системах із домінуючими ознаками романо-германського типу, до яких належить і правова система України, законодавство є основним інструментом регламентації важливих сфер суспільних відносин. Сьогодні інформаційна сфера стає визначальною для розвитку суспільства й держави, що визнано як багатьма міжнародними правовими актами, так і вітчизняним законодавством. Наміри стати правовою державою, задекларовані Конституцією України, ставлять на вищий щабель правові засади формування й реалізації державної політики за всіма напрямами. Серед них інформаційна політика набуває системоутворюючого характеру як важливий чинник формування національних ідеалів і цінностей, сприяння злагоді в суспільстві та консолідації зусиль на шляху суспільного розвитку, а отже, і забезпечення його безпеки.

У таких умовах законодавство (особливо концептуальна його складова) повинно ефективно виконувати не лише суто регламентаційні функції, а й ідеологічно-виховні, тобто створювати демократичну модель державної влади і зрозумілу для всіх відкриту концепцію державної політики.

Самоорганізаційні тенденції громадянського та інформаційного суспільства накладають певний відбиток як на функціональну спрямованість діяльності держави, так і на вибір методів та засобів здійснення державного впливу. Пріоритетним завданням держави стає забезпечення безпечних умов для розвитку суспільства загалом і кожної людини зокрема, що досягається виваженою державною політикою, інформаційна складова якої в сучасних умовах має вирішальне значення. Не останню роль у виконанні цього завдання відіграє якість інформаційного законодавства, формування якого є складним і водночас динамічним процесом.

Сьогодні інформаційна сфера України насичена численними несистематизованими нормативно-правовими актами з неоднозначним змістом, кількість яких із кожним роком зрос-

тає, що не сприяє ефективній їх реалізації, а отже, і досягненню режиму законності в інформаційній сфері, який є правовим виміром інформаційної безпеки.

Ще наприкінці 1990-х років за результатами досліджень Науково-дослідного центру правової інформатики Академії правових наук України із застосуванням комп'ютерної інформаційно-аналітичної системи «Законодавство» було визначено, що інформаційне законодавство становить значний масив нормативно-правових актів: понад 260 законів, 295 постанов Верховної Ради, 380 указів і 90 розпоряджень Президента, 1160 постанов і 210 розпоряджень Кабінету Міністрів, 1500 актів міністерств і відомств [342].

Звичайно, така ситуація не сприяє ефективному сприйняттю норм інформаційного законодавства, що вкрай негативно позначається на його дієвості й зумовлює значну активізацію досліджень, предметну частину яких становлять проблеми формування інформаційного права України, удосконалення вітчизняного інформаційного законодавства в умовах активного розвитку інформаційно-телекомунікаційних технологій і гармонійна адаптація його до міжнародних стандартів [194; 232].

Із метою виокремлення консолідованого погляду на концепцію розвитку інформаційного права України, виходячи з позиції достатньої дослідженості вітчизняними науковцями нормативно-правової бази сфери інформаційних відносин України, доцільним є аналіз їхніх висновків і зауважень, визначених проблем і шляхів їх вирішення з моменту актуалізації проблем інформаційного права. Деякі рекомендації науковців уже певним чином були реалізовані з прийняттям і вдосконаленням низки нормативно-правових актів, зокрема законів України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про державну таємницю», Доктрини інформаційної безпеки України тощо, проте окремі з визначених недоліків продовжують посилюватись.

Важливий внесок у розбудову правової системи України зробили українські науковці Р. А. Калюжний, В. С. Цимбалюк,

В. Д. Гавловський, М. В. Гуцалюк, які сформували цілісну систему поглядів на концептуальні основи інформаційного права України й проблеми його становлення. У 2001 році, пропонуючи та обґрунтовуючи шляхи систематизації інформаційного законодавства, вони акцентували увагу на проблемах, значна частина яких досі актуальна. Серед таких проблем:

– велика кількість законів і підзаконних нормативних актів у сфері інформаційних відносин, що ускладнює їх пошук, аналіз та реалізацію;

– неузгодженість понятійного апарату, спричинена різницею в часі прийняття законів та підзаконних актів, що регулюють суспільні відносини, об'єктом яких є інформація;

– термінологічні неточності, різне тлумачення однакових за назвою та формою понять і категорій, що призводить до їх неоднозначного розуміння і застосування на практиці;

– наявність розбіжностей щодо розуміння структури і складу системи законодавства у сфері інформаційних відносин і підходів до їх формування, що викликає дублювання норм та колізії в процесі їх реалізації;

– факти концептуальної неузгодженості нових правових актів у сфері суспільних інформаційних відносин із раніше прийнятими, що призводить до правового хаосу [234].

Серед важливих чинників процесу формування національного інформаційного права зазначені науковці підкреслили такі:

– необхідність і можливість виділення норм інформаційного права в окрему міжгалузеву інституцію з відповідною офіційною її систематизацією;

– відкритість питання формування доктрини, стратегії, концепції розвитку публічного права України у сфері суспільних інформаційних відносин;

– важливість вирішення питань правопорушень в інформаційній сфері, оскільки чинним інформаційним законодавством, поряд із диспозиціями таких правопорушень, санкції не встановлюються та не містяться посилання на відповідні акти, якими вони визначаються [119].

Для ефективного вирішення означених проблем було сформульовано систему вимог до правотворчого процесу в інформаційній сфері та змісту й структури інформаційного законодавства:

– методологія формування інформаційного законодавства повинна базуватися на положеннях теорії гіперсистем права, квінтесенція якої полягає в тому, що категорія «право» розглядається як велика, складна, багаторівнева, ієрархічна, соціальна система;

– системний і комплексний підходи у вирішенні проблем правотворчості; глибоке фундаментальне та прикладне теоретичне обґрунтування новацій (понять, категорій тощо);

– залучення широкого кола вітчизняних фахівців, які повинні володіти знаннями в галузі права та інформатики, бути обізнаними з досвідом зарубіжних країн, маючи при цьому своє, оригінальне, новаторське бачення вирішення проблем, виходячи зі специфіки реалій нашої країни;

– неприпустиме необґрунтоване копіювання зарубіжного досвіду;

– системоутворюючим чинником у національному інформаційному законодавстві повинен стати кодекс, який розвиватиме визначені в Конституції України положення інформаційних відносин, у тому числі щодо інформаційної безпеки, враховуватиме ратифіковані Україною нормативні акти (угоди, конвенції) міжнародного права [234].

Попри певні зміни законодавства України, досить актуальними сьогодні залишаються висновки І. В. Арістової, зроблені на початку періоду активізації досліджень вітчизняного інформаційного законодавства щодо можливостей його систематизації. Вона зазначає, що однією з найважливіших проблем на шляху створення інформаційного суспільства в Україні виступає формування і розвиток його правового фундаменту, основою якого є спеціальне інформаційне законодавство.

Ґрунтуючись на позиції, що стосовно галузевих юридичних наук теорія держави і права виступає як загальнотеоретич-

на, методологічна, базова наука, а її висновки і положення становлять основу вирішення спеціальних питань галузевих наук, І. В. Арістова наголошує на необхідності широкого підходу до правотворчості в інформаційній сфері. «Формування і розвиток українського інформаційного законодавства – це широкомасштабна діяльність, яка проникає так чи інакше в усі галузі права, охоплює правотворчість різноманітних владних органів держави і припускає участь у цьому процесі різних суб'єктів» [11, с. 196]. Для більш якісного здійснення такої діяльності необхідне проведення її за спеціальною державною програмою, в рамках певної інформаційно-правової політики. Тому одним із першочергових завдань повинне стати розроблення комплексної програми розвитку інформаційного законодавства, що визначатиме його склад і структуру, послідовність прийняття спеціальних законодавчих актів та окремих правових норм, які регулюватимуть весь комплекс інформаційних відносин. Пріоритети цієї програми мають видозмінюватися відповідно до об'єктивних змін інформаційної політики.

Перспективним, актуальним і своєчасним завданням інформаційної політики І. В. Арістова уважає кодифікацію інформаційного законодавства України, а в кінцевому рахунку – формування високої інформаційно-правової культури громадян, що є актуальним і для сьогодення [11].

Погоджуючись із думкою, що, по-перше, «інформаційне право» – це міжгалузевий комплексний інститут права, по-друге, за теорією гіперсистем його сформовано шляхом перерозподілу сфери нормативного регулювання між окремими галузями права [114, с. 124], Г. М. Красноступ стверджує, що галузь інформаційного законодавства вже сформована й однією з найактуальніших проблем є її удосконалення. Саме тому дуже важливо періодично проводити аналіз законодавства в цій сфері з метою його вчасного приведення у відповідність до потреб суспільства. Нині, на її думку, нам потрібно не створювати нові закони у сфері інформації, а систематизувати наявні, визначаючи в них правові гіперзв'язки, з метою їх подальшої кодифікації на рівні Кодексу України про інформацію. Кодекс «має чітко

визначити об'єкт, предмети інформаційного права, суб'єкти інформаційних правовідносин, правовий режим доступу до інформації, зокрема публічної (інформації органів державної влади та органів місцевого самоврядування), персональних даних, державної та іншої передбаченої законом таємниці» [150].

Широке коло актів інформаційного законодавства України й міжнародних актів, що стосуються інформаційної сфери, у світлі проблем правового доступу громадян до інформації розглянув А. І. Марущак, на основі чого зробив такі висновки:

– важливим напрямом розвитку кримінального права є розширення складів злочинів, які вчиняються з використанням новітніх інформаційних технологій, що в багатьох країнах називаються комп'ютерними злочинами (необхідно враховувати досягнення іноземних держав) [178, с. 383];

– нагальним є розроблення нормативно-правових актів різної юридичної сили, предметом регулювання яких були б правовідносини, пов'язані з інформаційними запитами як засобами доступу громадян до інформації, що сприятиме уніфікації та більш детальному правовому регулюванню такого доступу;

– необхідне вироблення правових принципів щодо платності (безоплатності) послуг із надання інформації, з урахуванням багатоманітності об'єктного та суб'єктного складів відповідних відносин;

– актуальною є проблема відсутності системного підходу до принципів і підстав обмеження доступу до інформації, повноважень відповідних суб'єктів щодо встановлення процедури (зокрема, умов та строків) такого обмеження, що викликає необхідність систематизації у вітчизняному праві виключних випадків обмеження права на доступ громадян до інформації, передбачених Конституцією України;

– обов'язок публічних суб'єктів, насамперед органів державної влади та їх посадових осіб, оприлюднювати певну інформацію не менш важливий, ніж задоволення інформаційних запитів громадян, оскільки відсутність повної, своєчасної та достовірної інформації може стати чинником виникнення багатьох негативних соціальних явищ;

– об'єктивно зумовлена недостатність науково-теоретичної розробленості чинної законодавчої бази щодо встановлення та притягнення до відповідальності за «комп'ютерні злочини» призводить до труднощів у практичній діяльності правоохоронних органів, суб'єктів господарювання тощо [178, с. 411–413].

Детальний аналіз базових нормативно-правових актів українського законодавства та правових актів Європейського Союзу, що регламентують інформаційні відносини з акцентуванням уваги на інформаційній безпеці, здійснений Ю. Є. Максименко. Обґрунтувавши загальний висновок про необхідність удосконалення українського інформаційного законодавства шляхом його кодифікації, дослідниця зокрема наголосила на такому:

– на правовому рівні інформаційна безпека має розглядатися в трьох аспектах – як інформаційно-психологічна безпека, інформаційна безпека у сфері прав та свобод, інформаційно-технічна безпека;

– позиція українського законодавця щодо нормативного розуміння інформаційної безпеки цілковито відповідає стандартам міжнародної спільноти і є більш повною та досконалою щодо європейського визначення поняття «інформаційна безпека», яке охоплює тільки інформаційно-технічний аспект;

– нормативно-правове регулювання інформаційно-психологічної безпеки та інформаційної безпеки у сфері прав і свобод де-юре відповідає міжнародним і європейським стандартам у цій сфері, причому здійснюється на рівні законів України;

– інформаційно-технічна безпека урегульована переважно підзаконними нормативно-правовими актами й потребує узгодження з європейськими стандартами;

– чітко простежується кількісний пріоритет нормативно-правових актів, спрямованих на врегулювання інформаційно-технічної безпеки щодо інформаційно-психологічної та інформаційної безпеки у сфері прав і свобод, що пов'язано, на думку дослідниці, з інтенсивним розвитком інформаційних техноло-

гій, а отже, необхідністю оперативного реагування на зміни певних стандартів у цій сфері;

– особливим недоліком нормативно-правового регулювання інформаційної безпеки України є його розпорошення в численних нормативно-правових актах різної юридичної сили, причому важливі проблеми нормативно закріплюються підзаконними нормативно-правовими актами;

– важлива проблема ефективного забезпечення інформаційної безпеки України – неузгодженість нормативно-правових актів як між собою, так і з чинною Конституцією, оскільки їх було прийнято ще до схвалення Основного Закону України;

– характерною рисою національного інформаційного законодавства є декларативність значного масиву норм без визначення шляхів їх реалізації, внаслідок чого спостерігається низький рівень реалізації норм права, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки;

– наразі наявні численні бланкетні чи відсильні норми права, значна кількість абстрактних, суб'єктивних понять, що потребують офіційного тлумачення або чіткого визначення, а також відсутнє закріплення фундаментальних, базових дефініцій (наприклад, інформаційної безпеки) [174].

На особливу увагу заслуговує позиція В. П. Горбуліна та М. М. Биченка, які, поряд із трансформаціями інформаційного законодавства, виокремлюють шляхи законодавчого удосконалення забезпечення інформаційної безпеки. Науковці підкреслюють потребу послідовної систематизації інформаційного законодавства. «По-перше, необхідно здійснити інкорпорацію існуючого інформаційного законодавства України і гармонізувати його з міжнародними стандартами. По-друге – започаткувати кодифікацію вітчизняного інформаційного законодавства, тобто його системне упорядкування» [66, с. 92].

Щодо пріоритетних заходів із вдосконалення й доповнення інформаційного законодавства України, то В. П. Горбулін та М. М. Биченок у 2008 році наголосили на необхідності:

– внесення змін до законів України «Про інформацію», «Про державну таємницю» з метою удосконалення термінології, що закріплюється цими законами, та приведення у відповідність зі стандартами розвинених країн доступу до державної таємниці;

– підготовки законодавчих актів «Про інформацію персонального характеру», «Про участь України в міжнародному інформаційному просторі» з метою врегулювання суспільних відносин, що виникають при збиранні, зберіганні, актуалізації, блокуванні, охороні та знищенні персональних даних, і створення умов для ефективних інформаційних взаємозв'язків України в глобальному світовому інформаційному просторі;

– законодавчого розмежування повноважень суб'єктів у сфері забезпечення інформаційної безпеки України; визначення цілей, функцій, завдань і механізмів участі в ній громадських об'єднань, організацій та громадян;

– уточнення правового статусу іноземних інформаційних агентств, засобів масової інформації й журналістів, а також інвесторів при залученні іноземних інвестицій для розвитку інформаційної інфраструктури України;

– визначення правового статусу організацій, що надають інформаційно-комунікаційні послуги на території України, і правового механізму регулювання їхньої діяльності;

– розвитку і вдосконалення нормативно-правового забезпечення комп'ютерно-телекомунікаційної безпеки, зокрема питання ліцензування діяльності у сфері інформатизації, сертифікації комп'ютерно-телекомунікаційних засобів, реалізації державного та громадського контролю і забезпечення інформаційної безпеки в межах передавання даних;

– законодавчого врегулювання суспільних відносин, що виникають у процесі обміну електронною інформацією, захисту певних видів інформації на машинних носіях, при формуванні та використанні національних інформаційних ресурсів;

– доцільності використання досвіду країн – членів ЄС, а також США і РФ із здійснення систематизації правових актів інформаційної сфери.

Важливим кроком на правовому шляху системного забезпечення інформаційної безпеки є розроблення конкретних цільових програм та планів дій щодо реалізації принципів єдиної інформаційної політики. До таких програм учені пропонують віднести програму стандартизації у сфері інформаційної безпеки, програму розвитку матеріально-технічного забезпечення інформаційної безпеки, програму науково-технічного і кадрового забезпечення інформаційної безпеки [66, с. 92–97].

Загалом із необхідністю систематизації українського інформаційного законодавства погоджуються всі дослідники цієї сфери. Серед них, не применшуючи внеску інших, можна згадати О. А. Баранова [20], К. І. Бєлякова [25], В. І. Бурковського [71], В. А. Ліпкана і В. А. Залізняка [163], які підтримують кодифікацію, та А. А. Письменицького [233], С. Е. Демського [245], що стояли на позиціях доцільності інкорпорації.

Важливим є також те, що кодифікація національних інформаційних законодавств визнана певним стандартом для країн СНД, а у 2008 році Міжпарламентською асамблеєю держав – учасниць СНД прийнято Модельний інформаційний кодекс держав – учасниць СНД [186].

Проаналізувавши позиції науковців щодо вдосконалення інформаційного законодавства України та особливості його сучасного стану, можна зробити низку узагальнень.

1. Обов’язковим науковим підґрунтям удосконалення законодавства в інформаційній сфері є з’ясування місця і структури інформаційного права у системі права України.

Щодо цієї проблеми єдиної позиції дослідників немає і виокремлюються три методологічні підходи:

1) інформаційне право в юридичній науці є міжгалузевою комплексною дисципліною. Об’єкт її дослідження – суспільні відносини, предметом яких виступає інформація; згідно з доктриною поділу права на галузі інформаційне право виявляється як міжгалузевий комплексний інститут між конституційним, адміністративним, цивільним, трудовим та кримінальним правом; інформаційне право тісно переплітається з іншими міжга-

лузевими комплексними інститутами: правом інтелектуальної власності, патентним правом на інтелектуальну промислову власність, авторським правом тощо [25, с. 264; 216, с. 56–57];

2) інформаційне право – це комплексна галузь права, яка регламентує суспільні відносини щодо інформації (форми відображення відомостей, повідомлень, даних, знань, сигналів), технологій її поширення, одержання та зберігання в усіх сферах життєдіяльності людини, що підлягають правовому регулюванню [337, с. 109];

3) інформаційне право може розглядатися як підгалузь наявних галузей права, зокрема цивільного й адміністративного, проте такі погляди більш притаманні початковому етапу розвитку інформаційного права [52; 145].

2. Попри те, що проблема систематизації інформаційного законодавства піднята науковцями понад десять років тому, суттєвих зрушень у напрямі її вирішення не відбулося. Різноманітні щорічні наукові форуми тільки підтверджують необхідність і актуальність систематизації, відзначаючи збільшення кола суспільних та правових проблем, які вона мала б вирішити [115]. Причиною такого становища є складний комплексний характер інформаційного права і законодавства. Зокрема, останнє, на думку Т. А. Костецької, з якою варто погодитись, – це розгалужена комплексна галузь, яку формують численні нормативно-правові акти різної юридичної сили – конституційного, адміністративного, цивільного, кримінального та інших галузей права, що регулюють відносини в інформаційній сфері [142, с. 8–9].

3. З огляду на комплексність інформаційного законодавства дещо сумнівним убачається уникнення в процесі його кодифікації бланкетних і відсильних норм, хоча кодифікація інформаційного права України, безперечно, позитивно позначиться на потенційних можливостях його сприйняття і дозволить внести необхідні зміни у фундаментальні правові акти інформаційної сфери.

Слід зазначити, що чіткі посилання в кодексі на інші нормативно-правові акти будуть створювати жорсткі системні

зв'язки, що в процесі подальшого вдосконалення зумовить необхідність системних змін положень усіх актів, пов'язаних такими посиланнями. Однак це об'єктивно спричинено динамікою інформаційної сфери, тому має сприйматися як необхідне.

Важливим під час кодифікації є використання методу агрегації: удосконалення окремих правових норм чи створення нових міжгалузевих правових інститутів не повинно порушувати цілісності та призначення законодавства, а навпаки, має покращувати, удосконалювати його дієвість у цілому, створювати нову системну якість, яка не притаманна окремим його складовим [41, с. 131–132].

Вирішенню проблем систематизації, з огляду на спільність типу правової системи, може сприяти аналіз німецького зразка інформаційного законодавства. У Німеччині інформаційне право є самостійною галуззю права, що поділяється на так звані підгалузі: інформаційного цивільного права, інформаційного кримінального права і права про адміністративні правопорушення; інформаційного цивільного права щодо електронно-інформаційних і комунікаційних послуг тощо [81, с. 170].

4. Дослідники концептуально-теоретичних основ інформаційної безпеки недостатньо уваги приділяють забезпеченості інформаційного законодавства охоронними нормами, часто не згадуючи норми кримінального та адміністративного права як правовий фундамент протидії загрозам в інформаційній сфері. Галузеві спеціалісти найчастіше займаються дослідженням та розвитком окремих інститутів інформаційного права в межах певної галузі. Зрештою це створює ситуацію певної неузгодженості як наукових досліджень, так і впровадження їх результатів у конкретну діяльність, що не сприяє ефективному вдосконаленню інформаційного законодавства України.

Отже, загалом слід підтримати визнану більшістю науковців ідею кодифікації інформаційного законодавства, оскільки вона є комплексним методом подолання багатьох перешкод, що стоять на шляху забезпечення законності й правопорядку в інформаційній сфері, а саме: переобтяжливої чисельності норма-

тивно-правових актів, дисгармонії понятійно-термінологічного апарату, суперечностей, прогалин у законодавстві, неузгодженості з міжнародними актами тощо.

Разом із тим, необхідно наголосити на деяких актуальних питаннях, вирішити які доцільно як безпосередньо в процесі кодифікації інформаційного законодавства, так і під час взаємопов'язаного з ним удосконалення і створення інших нормативно-правових актів.

По-перше, за умов низького рівня правосвідомості суспільства особливого значення набуває комплекс дієвих правових охоронних механізмів в інформаційній сфері, якому сьогодні українські законодавці не приділяють достатню увагу. Невирішеність означеної проблеми призводить до неповноти правового забезпечення і зниження ефективності правового впливу.

Безпрецедентне зростання цінності інформації підвищує суспільну шкоду від протиправних діянь в інформаційній сфері, що зумовлює необхідність переоцінки виду та міри юридичної відповідальності за них, особливо кримінальної. На жаль, кримінальне законодавство України є однією з найбільш сталих галузей законодавства, що не дозволяє йому на необхідному рівні охопити динамічні зміни суспільних цінностей і надати їм належного кримінально-правового захисту [261].

Справді, навіть поверховий аналіз основного акта кримінального законодавства України дозволяє зробити висновок про його «моральну застарілість» стосовно інституту відповідальності за злочини в інформаційній сфері. Це передусім виявляється в несформованості цього інституту в кримінальному праві України.

Так, Кримінальний кодекс України містить десятки статей, у яких інформацію можна розглядати як елементи складу злочину (об'єкт, предмет злочину, засіб його скоєння). Їх умовно можна поділити на декілька груп:

1) злочини, пов'язані з негативним інформаційно-психологічним впливом на суспільство та особу, – різноманітні небезпечні публічні заклики й агітація, розпалювання націона-

льної ворожнечі, пропаганда насильства і аморального способу життя, погрози різного характеру, примушення, спонукання, вимагання, схиляння, залякування;

2) злочини, пов'язані з таємною і конфіденційною інформацією, – шпигунство, незаконне збирання, передача й розголошення різного роду таємниць, незаконні дослідження, розголошення інформації про людину, порушення таємниці;

3) злочини, пов'язані з неналежним використанням або підміною інформації, – обман, шахрайство, неповідомлення, притягнення завідомо невинного до відповідальності, перешкоджання, фальсифікація, знищення, підробка, незаконне відтворення, зберігання, розповсюдження, приховування, викривлення інформації, надання завідомо неправдивої (недостовірної) інформації, ненадання інформації (відмова від надання інформації);

4) злочини, пов'язані з технічними засобами отримання та оброблення інформації.

Звичайно, наведений розподіл є достатньо умовним, проте розмаїття проявів протиправних «інформаційних діянь», представлених у ньому, певною мірою обґрунтовує необхідність уведення поняття «якість інформації» й додаткових досліджень у цьому напрямі. Якісна інформація має бути нешкідливою, повною, достовірною, своєчасно поширеною відповідно до рівня доступу до неї, а також суспільного значення. Розроблення методологічного підґрунтя визначення якості інформації може сприяти вирішенню на системному рівні деяких важливих проблем інформаційного законодавства.

По-друге, на сучасному етапі розвитку України все гостріше постають проблеми правового регулювання і забезпечення безпеки у сфері обміну та оброблення інформації, поданої у вигляді електронних комп'ютерних даних (кібернетична сфера). До найактуальніших із них належать:

– формування гармонійного правового понятійно-термінологічного апарату у сфері інформаційно-комунікаційних технологій (кіберсфері) [182];

– адаптація вітчизняного законодавства до міжнародних стандартів із протидії правопорушенням у сфері інформаційно-комунікаційних технологій з урахуванням можливостей України та особливостей її правової системи;

– виокремлення на рівні законодавства безпеки у сфері обміну та оброблення інформації у вигляді електронних комп'ютерних даних (кібербезпеки) як окремої складової інформаційної безпеки;

– удосконалення критеріїв віднесення об'єктів кібернетичної інфраструктури держави до тих, що мають критичне значення для безпеки держави, і створення правових засад їх захисту.

Для визначення ефективних шляхів удосконалення законодавства в цих напрямах особливо важливий правильний вибір засобів та методів правового регулювання. Як зазначають В. К. Шкарупа і В. С. Цимбалюк, «правове регулювання суспільних відносин в «е-середовищі» вимагає кореляції співвідношення методів адміністративного правового регулювання з методами цивільного та кримінального права й формування державної інформаційної політики, яку можна розглядати як державну політику інтелектуального розвитку людини, суспільства і держави» [353].

По-третє, суто кодифікація інформаційного законодавства України не вирішить проблем формування та відображення на нормативно-правовому рівні цілісної прозорої державної політики у сфері забезпечення інформаційної безпеки.

Інформаційна безпека – один із факторів подальшого розвитку суспільства і держави, що набуло визнання на концептуальному законодавчому рівні. Міжнародними актами вона визнається необхідним підґрунтям становлення інформаційного суспільства, яке є пріоритетом майбутнього і для України, що безпосередньо закріплено Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». Конституція України (ст. 17) забезпечення інформаційної безпеки відносить до найважливіших функцій держави поряд із захистом суверенітету і територіальної цілісності. Зако-

ном України «Про Концепцію Національної програми інформатизації» та Доктриною інформаційної безпеки України інформаційна безпека визначається як невід'ємна складова кожної зі сфер національної безпеки, причому Доктриною їй надається статус ще й важливої самостійної сфери забезпечення національної безпеки.

Незважаючи на це, увагу вітчизняного законодавця до інформаційної безпеки і проблем її забезпечення можна вважати ситуаційною. Україна наразі не має законодавчого акта, який відобразив би винятковість значення інформаційної безпеки й цілісні основи державної політики її забезпечення. Безперечним зрушенням у цьому напрямі є прийняття у 2009 році Указом Президента України Доктрини інформаційної безпеки України. Проте цей документ став результатом термінових, невідкладних заходів, що об'єктивно зумовило його певну недосконаліть, починаючи з відсутності дефініції інформаційної безпеки.

Отже, можна стверджувати, що сьогодні є необхідність системного удосконалення інформаційного законодавства України за такими трьома напрямами.

1. Кодифікація нормативно-правових актів інформаційного законодавства, що також визначено Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [255]. У процесі кодифікації, зважаючи на широту предметної сфери інформаційного законодавства, доцільним убачається обмеження змісту і сфери дії кодексу суспільними відносинами щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту різних видів інформації, а також особливостями здійснення різних видів інформаційної діяльності. Відповідно, однією з альтернативних його назв може бути «Кодекс України про інформацію та інформаційну діяльність». Необхідне також максимальне дотримання структури і загального стилю, традиційних для кодифікованих актів українського законодавства.

2. Удосконалення положень законодавства, які регламентують питання юридичної відповідальності за правопорушення в інформаційній сфері, насамперед кримінального, з метою приведення державно-правового реагування на найбільш небезпечні «інформаційні правопорушення» до об'єктивно необхідного рівня.

Зокрема, потрібно врахувати той факт, що сучасний кібернетичний простір (простір, сформований інформаційно-комунікаційними системами, в якому відбуваються процеси оброблення інформації, представленої у вигляді електронних комп'ютерних даних) надає широкі можливості використання його як знаряддя різних правопорушень, підвищуючи ефективність досягнення протиправних цілей. Це зумовлює транснаціональність, латентність, стрімкість, масштабність наслідків правопорушень, що загалом становить особливу суспільну небезпеку, яку не завжди можливо адекватно визначити.

Зазначене має знайти своє відображення в положеннях кримінального законодавства, зокрема, двома альтернативними шляхами: 1) доповнення низки статей частинами, які посилюють відповідальність за здійснення злочину з використанням інформаційно-комунікаційних систем, глобальних інформаційно-телекомунікаційних мереж тощо; 2) доповнення ст. 67 Кримінального кодексу України «Обставини, які обтяжують покарання» пунктом, який серед таких обставин передбачає використання інформаційно-комунікаційних систем, глобальних інформаційно-телекомунікаційних мереж тощо. Визначені шляхи потребують додаткового обговорення й вироблення консолідованої позиції відповідних спеціалістів, особливо у світлі новел Кримінального процесуального кодексу України щодо започаткування впровадження нового для правової системи України виду правопорушень – кримінального проступку, який у майбутньому матиме окрему регламентацію матеріальним кримінальним правом.

3. Формування комплексу нормативно-правових актів, що буде відображати цілісну модель державної політики забезпе-

чення інформаційної безпеки, зокрема прийняття Закону України «Про інформаційну безпеку України». Такий Закон повинен формуватися на спільній методологічній основі із Законом України «Про основи національної безпеки України», деталізувати його положення щодо інформаційної безпеки та основних засад державної політики її забезпечення і сприяти виконанню завдань:

– визначення поняття і змісту інформаційної безпеки в контексті розвитку інформаційного суспільства в Україні;

– відображення інформаційної безпеки в усіх її аспектах, важливих для державно-правового забезпечення;

– розкриття особливостей об'єктів інформаційної безпеки;

– деталізації національних інтересів в інформаційній сфері;

– затвердження принципів забезпечення інформаційної безпеки з урахуванням аспектів її розуміння;

– визначення узагальнених загроз інформаційній безпеці за сферами національної безпеки;

– окреслення основних напрямів державної політики з питань інформаційної безпеки як самостійної сфери і за сферами національної безпеки;

– визначення суб'єктів забезпечення інформаційної безпеки та загальних особливостей їх повноважень;

– створення правового підґрунтя для формування відповідних підзаконних актів, зокрема доктрин, стратегій та програм забезпечення інформаційної безпеки загальнодержавного, регіонального, галузевого й іншого значення.

ВИСНОВКИ

Початок третього тисячоліття ознаменований масштабним переходом до нової концепції розвитку – глобального інформаційного суспільства. Інформація стає цінним ресурсом знань, інструментом розвитку, до якого кожен повинен мати повноцінний доступ.

Держави, які знаходяться в авангарді інформаційного розвитку, докладають зусиль у подоланні інформаційної нерівності як між країнами, так і серед окремих осіб, та утвердженні визнаних Загальною декларацією прав людини загальнолюдських цінностей свободи, справедливості, злагоди.

Україна не стоїть осторонь цих процесів, намагається брати в них посильну участь та поступово входити до світового інформаційного простору як повноправний його учасник.

Проте інтенсивний інформаційний розвиток, що спричиняє проникнення інформаційно-комунікаційних технологій в усі сфери суспільного життя, крім значного потенціалу для самоорганізації та самореалізації, несе низку нових загроз глобального масштабу, серед яких – кіберзлочинність і кібертероризм, розмивання національної ідентичності, нехтування моральними засадами суспільства, маніпулювання свідомістю.

У таких умовах стратегічного значення набуває виважена інформаційна політика держави, що виводить на перший план функцію забезпечення інформаційної безпеки, а спрямованість на розбудову правової держави зумовлює пріоритетність правових форм і методів її реалізації.

Отже, теоретико-правове дослідження інформаційної безпеки та її забезпечення, зокрема державно-правової складової, є актуальним і необхідним.

Вибір і адаптація розроблених наукою методологічних підходів, серед яких для дослідження інформаційної безпеки як функції держави домінуюче значення мають діяльнісний, функціональний, системний, класифікаційний підходи, орієнтують на таке:

1) варіативність осмислення інформаційної безпеки та її забезпечення як систем зумовлена тим, що вони, маючи власні

підсистеми, можуть розглядатися підсистемами інших систем, зокрема, державної, правової, національної безпеки тощо; причому, як підсистеми, інформаційна безпека та її забезпечення набувають своєрідних властивостей, зумовлених природою тих систем, до складу яких вони входять;

2) у державній системі переважного значення набувають характеристики забезпечення інформаційної безпеки як державної діяльності, функції держави загалом і кожного з її органів окремо; у системі національної безпеки – як протидії загрозам національній безпеці в інформаційній сфері, створення умов для безпечного існування людини, суспільства, держави в інформаційному середовищі; у правовій системі – як правових форм її здійснення, особливостей правового регулювання, правових гарантій, законності (правності);

3) кожна з підсистем державно-правового забезпечення інформаційної безпеки повинна осмислюватися як система, зокрема, державної діяльності, нормативно-правових актів, суб'єктів забезпечення, засобів і методів, керівних принципів тощо;

4) діяльнісний вимір як інформаційної безпеки та її забезпечення загалом, так і їх окремих аспектів, у поєднанні із системним підходом сприятиме формуванню цілісної галузі знань про сучасну інформаційну безпеку, яка буде відображати природні риси цього феномену, серед яких:

– варіативність проявів, зокрема невід'ємність таких із них, як інформаційно-технічна, інформаційно-правова, інформаційно-психологічна безпека;

– зверхність гуманістичної парадигми інформаційної безпеки над техніко-технологічною, що орієнтує на пріоритетність задоволення потреб й інтересів людини і суспільства;

– діалектичність інформаційного середовища, що відображає суб'єктивність оптимального поєднання позитивних і негативних чинників, необхідних для стабільного інформаційного розвитку;

– нерозривність взаємозв'язку з інформаційним суспільством як метою і результатом діяльності із забезпечення інформаційної безпеки;

– синергетичність інформаційної безпеки, що зумовлює невід'ємність самоорганізаційної складової забезпечення інформаційної безпеки;

– субсидіарність у співвідношенні державного й недержавного забезпечення, яка визначає межі втручання держави в процеси забезпечення інформаційної безпеки людини і суспільства;

– комплексність у виборі засобів і методів забезпечення інформаційної безпеки, що забезпечує його повноту й оптимальність результатів;

– глобальність, транснаціональність, консолідованість забезпечення інформаційної безпеки в процесі розбудови глобального інформаційного суспільства і повноцінного входження всіх членів світового суспільства у світовий інформаційний простір.

Правовим відображенням належного рівня інформаційної безпеки є сукупність правових умов, що забезпечують оптимальне функціонування й розвиток суб'єктів в інформаційному середовищі, складовою якого, як однією з форм буття права, виступає інформація про можливе, належне, заборонене в людській поведінці. Звідси можливе уведення поняття «інформаційно-правова безпека» й асоціювання його з режимом законності (правності) в інформаційній сфері, а також розгляд правової інформації як особливого предмета інформаційних відносин, універсального організаційного засобу, який є важливим інструментом державного забезпечення інформаційної безпеки і, водночас, об'єктом захисту.

Якість правової інформації та можливості її належного обігу визначають результативність правового забезпечення інформаційної безпеки й мають підвищуватися за рахунок широкого використання сучасних інформаційно-комунікаційних технологій.

Законність (правність) є необхідним організаційно-ідеологічним фундаментом досягнення таких високих цілей, як розвиток громадянського та інформаційного суспільства й розбудова правової держави. Законність (правність) в інформацій-

ній сфері життя суспільства і держави активно сприятиме цим процесам та забезпечуватиме стабільний інформаційний розвиток суспільства, ефективну взаємодію членів суспільства між собою і з державою, що в сутності є метою забезпечення інформаційної безпеки.

Юридичними гарантіями законності (правності) в інформаційній сфері є ефективне дієве інформаційне законодавство, яке повинно відповідати низці вимог, серед яких:

– забезпеченість на рівні концепцій, принципів, дефініцій, що відображають багатоаспектність інформаційної безпеки;

– високий рівень законодавчої техніки й термінологічний комплекс, що відповідає усім вимогам до мови закону та юридичної термінології;

– зручність інформаційного законодавства;

– передбачуваність ефективних механізмів реалізації;

– розвиненість і виваженість інституту юридичної відповідальності за правопорушення в інформаційній сфері;

– адекватне відображення в інформаційному законодавстві реальних умов життя, міжнародних стандартів, напрямів розвитку суспільства, балансу інтересів держави, суспільства та особи.

Слід визнати, що зміст концептуальних положень інформаційного законодавства України відповідає міжнародним стандартам, проте повною мірою вони не реалізуються. Одна з причин цього – недосконалість інформаційного законодавства, яка об’єктивно зумовлена становленням інформаційного права і правової системи України загалом. Серед напрямів поліпшення ситуації – кодифікація основних нормативно-правових актів, що регламентують відносини, пов’язані з інформацією та інформаційною діяльністю; удосконалення законодавства, яке регламентує питання юридичної відповідальності за правопорушення в інформаційній сфері, передусім кримінального; формування комплексу нормативно-правових актів, що відображатимуть цілісну прозору модель державної політики забезпечення інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» / Д. С. Азаров. − К., 2003. − 18 с.

2. Азизов Р. Ф. Правовая информация: теоретические аспекты понимания и особенности законодательного закрепления / Р. Ф. Азизов // История государства и права. − 2007. − № 4. − С. 31−35.

3. Алексеев С. С. Общая теория права : в 2-х т. / С. С. Алексеев. − М. : Юрид. лит., 1981. − Т. 1. − 360 с.

4. Алексеев С. С. Правовые средства : постановка проблемы, понятия, классификация / С. С. Алексеев // Советское государство и право. − 1987. − № 6. − С. 12−19.

5. Алексеев С. С. Проблемы теории государства и права / С. С. Алексеев. − М., 1987. − 448 с.

6. Алексеева И. Ю. Возникновение идеологии информационного общества [Електронний ресурс] : Распределенная конференция «Технологии информационного общества 98 − Россия» / И. Ю. Алексеева. − Режим доступу : http://www.iis.ru/events/19981130/alexeeva.ru.html

7. Андреева Г. М. Социальная психология : учеб. / Г. М. Андреева. − М. : Аспект Пресс, 2001. − 378 с.

8. Андрєєва О. М. Національна безпека України в контексті національної ідентичності і взаємовідносин з Росією : автореф. дис. на здобуття наук. ступеня докт. політ. наук : спец. 23.00.01 «Теорія та історія політичної науки» / О. М. Андрєєва. − К., 2010. − 36 с.

9. Анисимова Н. В. Принцип субсидиарности в европейском праве : дис. … канд. юрид. наук : 12.00.10 / Н. В. Анисимова. − М., 2005. − 173 с.

10. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і

процес; фінансове право; інформаційне право» / І. В. Арістова. − Х., 2002. − 39 с.

11. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти : монографія / І. В. Арістова ; [заг. ред. О. М. Бандурка]. − Х. : Вид-во Ун-ту внутр. справ, 2000. − 368 с.

12. Ароян А. С. Субсидиарность как концептуальная основа эффективного взаимодействия государства, местного самоуправления и гражданского общества : дис. … канд. полит. наук : 23.00.01 / А. С. Ароян. − Ростов-на-Дону, 2010. − 185 с.

13. Артамонова Я. С. Информационная безопасность и социальный конфликт в современной России : дис. ... канд. социол. наук : 22.00.04 / Я. С. Артамонова. − Волгоград, 2006. − 182 с.

14. Архипова Є. О. Інформаційна безпека : соціально-філософський вимір : автореф. дис. на здобуття наук. ступеня канд. філософ. наук : спец. 09.00.03 «Соціальна філософія та філософія історії» / Є. О. Архипова. − К., 2012. − 21 с.

15. Атаманов Г. А. Информационная безопасность в современном российском обществе (Социально-философский аспект) : дис. ... канд. филос. наук : 09.00.11 / Г. А. Атаманов. − Волгоград, 2006. − 168 с.

16. Атаян Г. Ю. Экономическая функция российского государства : дис. ... канд. юрид. наук : 12.00.01 / Г. Ю. Атаян. − Ставрополь, 2006. − 214 с.

17. Бабаев С. В. Теория функций современного российского государства : дис. ... канд. юрид. наук : 12.00.01 / С. В. Бабаев. − Н. Новгород, 2001. − 201 с.

18. Байтин М. И. Сущность и основные функции социалистического государства / М. И. Байтин. − Саратов : Изд-во Сарат. ун-та, 1979. − 302 с.

19. Балдицын В. В. Охранительные правоотношения в сфере обеспечения информационной безопасности современной России (Теоретико-правовой аспект) : дис. ... канд. юрид. наук : 12.00.01 / В. В. Балдицын. − СПб., 2000. − 178 с.

20. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи / О. А. Баранов. − К. : Видавничий дім «СофтПрес», 2005. − 316 с.

21. Бебик В. М. Глобальне інформаційне суспільство: поняття, структура, комунікації / В. М. Бебик // Інформація і право. − 2011. − № 1 (1). − С. 41−49.

22. Бекетов Н. Информационная безопасность развития государства / Н. Бекетов // Информационные ресурсы России. − 2004.− № 6. − С. 32−35.

23. Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / Д. Белл ; [пер. с англ. под ред. В. Л. Иноземцева]. – М., 1999. – 783 с.

24. Бєляков К. І. Правова інформація як складова правової реальності / К. І. Бєляков // Часопис Київського університету права. – 2005. – № 1. – С. 22–27.

25. Беляков К. И. Управление и право в период информатизации : монография / К. И. Беляков. − К. : Издательство «КВІЦ», 2001. − 301 с.

26. Березовська І. Р. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні : дис. ... канд. юрид. наук : 12.00.07 / І. Р. Березовська. − К., 2012. − 239 с.

27. Берлач А. І. Основи економічної безпеки України : навч. посібник / А. І. Берлач, Т. В. Філіпенко. − Донецьк : Донецький юридичний інститут, 2007. − 420 с.

28. Бермічева О. В. Соціальна функція держави в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / О. В. Бермічева. − Х., 2002. − 18 с.

29. Бернюков А. М. Юридична герменевтика як методологія здійснення правосуддя (філософсько-теоретичний аналіз) : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.12 «Філософія права» / А. М. Бернюков. − Л., 2008. − 16 с.

30. Бєляков К. І. Організаційно-правове та наукове забезпечення інформатизації в Україні: проблеми теорії та практики : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / К. І. Бєляков. − К., 2009. − 38 с.

31. Білоусов А. С. Криміналістичний аналіз об’єктів комп’ютерних злочинів : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та

криміналістика; судова експертиза; оперативно-розшукова діяльність» / А. С. Білоусов. − К., 2008. − 19 с.

32. Бірюков В. В. Використання комп'ютерних технологій для фіксації криміналістично значимої інформації у процесі розслідування : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / В. В. Бірюков. − К., 2001. − 20 с.

33. Бобровник С. В. Законність / С. В. Бобровник // Великий енциклопедичний юридичний словник / [ред. Ю. С. Шемшученко]. − К. : Юрид. думка, 2007. − С. 274.

34. Богданова М. А. Теоретические аспекты совершенствования государственной политики развития информационного пространства и обеспечения информационной безопасности России в современных условиях : дис. ... канд. полит. наук : 23.00.02 / М. А. Богданова. − М., 2006. − 143 с.

35. Боер В. М. Информационно-правовая политика и безопасность России: Теоретико-правовой аспект : автореф. дисс. на соискание учен. степени докт. юрид. наук : 12.00.01 / В. М. Боер. − СПб., 1998. − 15 с.

36. Большой энциклопедический словарь. − 2-е изд. перераб. и доп. − М. : «Большая Российская энциклопедия», 1997. − 1456 с.

37. Борисов А. Ю. Государственная политика в области информационной безопасности на современном этапе : дис. ... канд. полит. наук : 23.00.02 / А. Ю. Борисов − М., 2006. − 166 с.

38. Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / Л. В. Борисова. − К., 2007. − 19 с.

39. Брижко В. М. До гносеології категорії «інформація» / В. М. Брижко // Інформація і право. − 2011. − № 2 (2). − С. 13−20.

40. Брижко В. М. Організаційно-правові питання захисту персональних даних : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і про-

цес; фінансове право; інформаційне право» / В. М. Брижко. − Ірпінь, 2004. − 20 с.

41. Брижко В. М. Вступ до інформаційної культури та інформаційного права / В. М. Брижко, В. Д. Гавловський, Р. А. Калюжний та ін. ; [заг. ред. М. Я. Швець, Р. А. Калюжний]. − Ужгород : ІВА, 2003. − 240 с.

42. Бурило Ю. П. Організаційно-правові питання державного управління в інформаційній сфері : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Ю. П. Бурило. − К., 2008. − 18 с.

43. Бусленко Н. И. Политико-правовые основы обеспечения информационной безопасности Российской Федерации в условиях демократических реформ : дис. ... докт. полит. наук : 23.00.02 / Н. И. Бусленко. − Ростов-на-Дону, 2003. − 439 с.

44. Бухтерева М. А. Формы реализации функций государства : дис. ... канд. юрид. наук : 12.00.01 / М. А. Бухтерева. − М., 2002. − 202 с.

45. Варич О. Г. Економічні функції сучасної держави: природа, зміст, тенденції розвитку в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / О. Г. Варич. − К., 2006. − 20 с.

46. Васенина А. Н. Информационная функция современного Российского государства : дис. ... канд. юрид. наук : 12.00.01 / А. Н. Васенина. − Н. Новгород, 2008. − 218 с.

47. Василюк В. Я. Інформаційна безпека держави : курс лекцій / В. Я. Василюк, С. О. Климчук. − К. : КНТ, Видавничий дім «Скіф», 2008. − 136 с.

48. Ващинець І. І. Цивільно-правова охорона авторських прав в умовах розвитку інформаційних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / І. І. Ващинець. − К., 2006. − 20 с.

49. Введение в теорию государственно-правовой организации социальных систем / [общ. ред. Е. Б. Кубко]. − К. : Юринком, 1997. − 192 с.

50. Великий тлумачний словник сучасної української мови (з дод. і допов.) / [уклад. і голов. ред. В. Т. Бусел]. − К.; Ірпінь : ВТФ «Перун», 2005. − 1728 с.

51. Венгеров А. Б. Теория государства и права : учеб. для юрид. вузов / А. Б. Венгеров. − 3-е изд. − М. : Юриспруденция, 2000. − 528 с.

52. Виноградова Г. В. Правове регулювання інформаційних відносин в Україні / Г. В. Виноградова. − К. : «Юстініан», 2006. − 463 с.

53. Воротилина Т. Л. Постнеклассические тенденции в западной и российской традициях правопонимания : дис. ... канд. юрид. наук : 12.00.01 / Т. Л. Воротилина. − Н. Новгород, 2002. − 228 с.

54. Всемирная встреча на высшем уровне по вопросам информационного общества (Женева, 2003 г. − Тунис, 2005 г.) Декларация принципов. Документ WSIS−03/GENEVA/DOC/4−R от 12 декабря 2003 года [Електронний ресурс]. − Режим доступу : http://www.un.org/russian/conferen/wsis/dec.pdf

55. Всемирная встреча на высшем уровне по вопросам информационного общества (Женева, 2003 г. − Тунис, 2005 г.). План действий. Документ WSIS-03/GENEVA/DOC/5-R от 12 декабря 2003 года [Електронний ресурс]. − Режим доступу : http://www.un.org/russian/conferen/wsis/plan.pdf

56. Всемирная встреча на высшем уровне по вопросам информационного общества (Женева, 2003 г. − Тунис, 2005 г.). Тунисское обязательство. Документ WSIS-05/TUNIS/DOC/7-R от 15 ноября 2005 года [Електронний ресурс]. − Режим доступу : http://www.un.org/russian/conferen/wsis/commitment.pdf

57. Всемирная встреча на высшем уровне по вопросам информационного общества (Женева, 2003 г. − Тунис, 2005 г.). Тунисская программа для информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R от 15 ноября 2005 года [Електронний ресурс]. − Режим доступу : http://www.nbuv.gov.ua/law/05tunis2.pdf

58. Всемирный саммит по информационному обществу : ЮНЕСКО отстаивает свободу слова. Париж, декабрь 2003 г. [Електронний ресурс]. − Режим доступу : http://www.unesco.org/bpi/rus/pdf/03-102-Russe.pdf

59. Ганьба Б. П. Системний підхід та його застосування в дослідженні України як демократичної, соціальної, правової держави : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / Б. П. Ганьба. − Х., 2001. − 19 с.

60. Гладенко О. М. Міжнародно-правове співробітництво України з Європейським Союзом у сфері Спільної зовнішньої політики та політичної безпеки : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.11 «Міжнародне право» / О. М. Гладенко. − О., 2010. − 21 с.

61. Гладышев А. Г. Основы социального управления : учеб. пособие / А. Г. Гладышев, В. Н. Иванов, В. И. Патрушев и др. ; [ред. В. Н. Иванов]. − М. : Высш. шк., 2001. − 271 с.

62. Глебов А. П. Понятие и структура функций социалистического государства: пособие по спецкурсу «Проблемы теории социалистического государства и права» / А. П. Глебов. − Воронеж, 1974. − 150 с.

63. Глебов А. П. К теории функций государства / А. П. Глебов // Каск Л. И. Функции и структура государства / Л. И. Каск. − Л. : Изд. ЛГУ, 1969. − 64 с.

64. Голобуцький О. «Електронний уряд» [Електронний ресурс] / О. Голобуцький, О. Шевчук. − Режим доступу : http://golob.narod.ru/egovper.html

65. Горбулін В. Актуальні проблеми системного забезпечення інформаційної безпеки України / В. Горбулін, М. Биченок, П. Копка // Форми та методи забезпечення інформаційної безпеки держави : зб. матеріалів наук.-практ. конф. (м. Київ, 13 березня 2008 р.). − К. : Видавець Захаренко В. О., 2008. − 216 с.

66. Горбулін В. П. Проблеми захисту інформаційного простору України : монографія / В. П. Горбулін, М. М. Биченок. − К. : Інтертехнологія, 2009. − 136 с.

67. Горінецький Й. І. Правоохоронна функція держав Центральної Європи: теоретичні і практичні аспекти : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / Й. І. Горінецький. − К., 2005. − 20 с.

68. ГОСТ Р ИСО/МЭК 17799 «Информационные технологии. Практические правила управления информационной безопасностью» [Електронний ресурс]. − Режим доступу : http://www.npo-echelon.ru/common_files/gost/GOST-17799-2005.pdf

69. ГОСТ Р ИСО/МЭК 27001 «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования» [Електронний ресурс]. − Режим доступу : http://www.altell.ru/assets/images/laws/standard/27001-2006.pdf

70. Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г. В. Грачев. − М. : Изд-во РАГС, 1998. − 125 с.

71. Гурковський В. І. Державне управління розбудовою інформаційного суспільства в Україні (історія, теорія, практика) / В. І. Гурковський. − К. : «Видавництво «Науковий світ» та МНДЦ з проблем боротьби з організованою злочинністю при РНБО України, 2010. − 396 с.

72. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки : дис. … канд. юрид. наук : 25.00.02 / В. І. Гурковський. − К., 2004. − 225 с.

73. Гусарєв С. Д. Функціональний підхід та функції юридичної практичної діяльності / С. Д. Гусарєв // Держава і право: збірник наукових праць. Юридичні і політичні науки. − К. : Ін-т держави і права ім. В.М. Корецького НАН України, 2005. − Вип. 30. − С. 55−60.

74. Гусарєв С. Д. Юридична діяльність: методологічні та теоретичні аспекти / С. Д. Гусарєв. − К. : Знання, 2005. − 375 с.

75. Давыдов А. А. Системная социология / А.А. Давыдов. – 2-е изд. − М. : Издательство ЛКИ, 2008. − 192 с.

76. Данільян О. Г. Національна безпека України: сутність, структура та напрямки реалізації / О. Г. Данільян, О. П. Дзьобань, М. І. Панов. − Х. : «ФОЛІО», 2002. − 296 с.

77. Декларация о культуре мира и программа действий в области культуры мира. Утверждены резолюцией 53/243 Генеральной Ассамблеи ООН от 13 сентября 1999 года [Електрон-

ний ресурс]. − Режим доступу : http://www.un.org/russian /documen/declarat/ culture_ of_peace.pdf

78. Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом ООН. Утверждена резолюцией 2625 (XXVI) Генеральной Ассамблеи ООН от 24 октября 1970 года [Електронний ресурс]. − Режим доступу : http://www.un.org/russian/documen/gadocs/convres/r25-2625.pdf

79. Декларация принципов терпимости. Утверждена резолюцией 5.61 Генеральной конференции ЮНЕСКО от 16 ноября 1995 г. [Електронний ресурс]. − Режим доступу : http://www.un.org/russian/documen/declarat/toleranc.htm

80. Декларация тысячелетия Организации Объединенных Наций. Утверждена резолюцией 55/2 Генеральной Ассамблеи ООН от 8 сентября 2000 г. − [Електронний ресурс]. − Режим доступу : http://www.un.org/russian/documen/gadocs/ convres/r15-1514.pdf

81. Демкова М. Інформаційне право: стан та перспективи розвитку в Україні (з «круглого столу») / М. Демкова // Право України. − 2004. − № 5. − С. 169−171.

82. Денисов А. И. Советское государство: возникновение, развитие, сущность и функции / А. И. Денисов − М. : Моск. гос. ун-т, 1967. − 427 с.

83. Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посіб. / О. О. Денісова. − К. : КНЕУ, 2003. − 315 с.

84. Украинская советская энциклопедия − К. : Главная редакция Украинской Советской Энциклопедии, 1980. − Т. 3. − 544 с.

85. Джураєва О. О. Функції сучасної держави : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / О. О. Джураєва. − О., 2006. − 20 с.

86. Дзіс С. А. Проблеми авторського права в сфері новітніх комп’ютерних технологій : дис. … канд. юрид. наук : 12.00.03 / С. А. Дзіс. − К., 2004. − 252 с.

87. Дмитренко В. А. О методологическом значении деятельностного подхода к науке / В. А. Дмитренко // Вопросы методологии наук. − 1975. – Вып. 5. − С. 3−20.

88. Дмитришин В. С. Набуття та передання авторських прав на комп'ютерні програми : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / В. С. Дмитришин. − К., 2008. − 20 с.

89. Доктрина информационной безопасности Российской Федерации [Електронний ресурс]. − Режим доступу : http://www.mid.ru/bdomp/ns-osndoc.nsf/d06bd3f5303124fe432569fa003a70ff/4db2749a4b55f02f432569fb004872a4!OpenDocument

90. Доценко Е. Л. Психология манипуляции: феномены, механизмы и защита / Е. Л. Доценко. − М. : ЧеРо, Издательство МГУ, 1997. − 344 с.

91. Дудаш Т. І. Праворозуміння: герменевтичне дослідження : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / Т. І. Дудаш. − Л., 2008. − 16 с.

92. Дьяконов В. В. Контроль и надзор в системе функций государства (Теоретический аспект) : дис. ... канд. юрид. наук : 12.00.01 / В. В. Дьяконов. − М., 2006. − 209 с.

93. Еллинек Г. Общее учение о государстве / Г. Еллинек. − СПб., 1908. − 570 с.

94. Емелин В. Постмодернизм и информационные технологии [Електронний ресурс] / В. Емелин. − Режим доступу : http://www.geocities.com
/emelin_vadim/articles.htm

95. Емельянов Г. В. Проблемы обеспечения информационно-психологической безопасности России [Електронний ресурс] / Г. В. Емельянов, В. Е. Лепский, А. А. Стрельцов // Информационное общество. − 1999. − № 3. − С. 47−51. − Режим доступу : http://www.reflexion.ru/Library/Lepsky_1999_d.htm

96. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : дис. ... канд. наук з держ. упр. : 25.00.01 / Л. О. Євдоченко. − Львів, 2011. − 225 с.

97. Єзеров А. А. Конституційний конфлікт як феномен та процес в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.02 «Конституційне право; муніципальне право» / А. А. Єзеров. − О., 2007. − 18 с.

98. Жоль К. К. Методы научного познания и логика (для юристов) : учеб. пособие / К. К. Жоль. − К. : Атика, 2001. − 288 с.

99. Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / А. І. Журба. − Х., 2008. − 19 с.

100. Загальна декларація прав людини. Прийнята і проголошена резолюцією 217А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

101. Загальна теорія держави і права / [ред. В. В. Копєйчиков]. − К. : Юрінком, 1997. − 320 с.

102. Загидуллин Р. И. Правоохранительная функция современного российского государства (Вопросы теории и практики) : дис. ... канд. юрид. наук : 12.00.01 / Р. И. Загидуллин. − Уфа, 2004. − 184 с.

103. Заінчковський М. Л. Права людини як новоєвропейський філософський та політико-правовий феномен : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.12 «Філософія права» / М. Л. Заінчковський. − К., 2003. − 20 с.

104. Залєвська І. І. Інформаційна безпека України в сучасних умовах: політичний аспект : дис. ... канд. політ. наук : 23.00.02 / І. І. Залєвська. − Одеса, 2012. − 177 с.

105. Залєвська І. І. Принципи державної політики у сфері забезпечення інформаційної безпеки [Електронний ресурс] / І. І. Залєвська // Вісник ДАКККіМ. − 2011. − № 1. − Режим доступу : http://www.nbuv.gov.ua/portal/Soc_Gum/Vdakk/2011_1/46.pdf

106. Захаров М. Ю. Информационная безопасность социума: социально-философское исследование / М. Ю. Захаров. − Ростов-на-Дону, 1998. − 258 с.

107. Звід правил для управління інформаційною безпекою. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 [Електронний ресурс]. −

Режим доступу : http://www.bank.gov.ua/B_zakon/Draft/02022010/27002.pdf

108. Иванов Д. Идея Информационного общества и Internet [Електронний ресурс] / Д. Иванов. − Режим доступу : http://www.soc.pu.ru:8101/persons/dvi/internet.html

109. Иванов С. И. Виртуальность / С. И. Иванов. − М. : 2006. − 187 с.

110. Иващенко Г. В. Доктрина информационной безопасности и методологические проблемы теории безопасности / Г. В. Иващенко // Глобальная информатизация и безопасность Росии / [общ. ред. В. И. Дебреньков]. − М : Изд-во Московского университета, 2001. − 398 с.

111. Иноземцев В. Л. Современное постиндустриальное общество: природа, противоречия, перспективы : учеб. пособие для студ. вузов / В. Л. Иноземцев. − М. : Логос, 2000. − 304 с.

112. История стандарта BS 7799 [Електронний ресурс] : ISO27000.ru. − Режим доступу : http://www.iso27000.ru/chitalnyi-zai/standarty-informacionnoi-bezopasnosti/istoriya-standarta-bs-7799

113. Іванов Д. А. Інформаційно-правові основи забезпечення безпеки мореплавства : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Д. А. Іванов. − О., 2008. − 19 с.

114. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії та практики : монографія / [ред. Р. А. Калюжний, В. О. Шамрай]. − К., 2002. − 296 с.

115. Інформаційне законодавство України: проблеми і перспективи [Електронний ресурс]. − Режим доступу : http://instzak.rada.gov.ua/instzak/doccatalog/document?id=46630

116. Кадомцева А. Е. Развитие экологической функции современного Российского государства и правовые формы ее осуществления : дис. ... канд. юрид. наук : 12.00.01 / А. Е. Кадомцева. − Саратов, 1999. − 174 с.

117. Казимирчук В. П. Право и методы его изучения / В. П. Казимирчук. − М. : Юрид. лит., 1965. − 204 с.

118. Каландаров К. Х. Управление общественным сознанием. Роль коммуникативных процессов / К. Х. Каландаров. − М. : Гуманитарный центр «Монолит», 1998. − 80 с.

119. Калюжний Р. А. Інформаційному суспільству України інформаційне законодавство (Щодо питань реформування законодавства у сфері суспільних інформаційних відносин) [Електронний ресурс] : Центр информационной безопасности / Р. А. Калюжний, В. С. Цимбалюк, В. Д. Гавловський, М. В. Гуцалюк. − Режим доступу : http://www.bezpeka.com /ru/lib/spec/law/ukraine-information-society-legislation.html

120. Каракулян Э. А. Идея субсидиарности в истории правовых учений: личность, общество, государство (Теоретико-правовой анализ) : дис. ... канд. юрид. наук : 12.00.01 / Э. А. Каракулян. − Н. Новгород, 2004. − 219 с.

121. Карпова Н. А. Правоохранительная функция правового государства : дис. ... канд. юрид. наук : 12.00.01 / Н. А. Карпова. − М., 2007. − 159 с.

122. Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину) : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» / М. В. Карчевський. − Х., 2003. − 19 с.

123. Каск Л. И. Функции и структура государства / Л. И. Каск. − Л. : Изд–во Ленинград. ун-та, 1969. − 65 с.

124. Кастельс М. Информационная эпоха. Экономика, общество и культура [Електронний ресурс] : Библиотека Гумер / М. Кастельс. − Режим доступу : http://www.gumer.info /bibliotek_Buks/Polit/kastel/index.php

125. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А. Б. Качинський. − К., 2003. − 472 с.

126. Киреева С. А. Межгосударственная интеграция как внешняя функция Российского государства : дис. ... докт. юрид. наук : 12.00.01 / С. А. Киреева. − Астрахань, 2006. − 499 с.

127. Клочко А. А. Эволюция социальных функций государства : дис. ... канд. экон. наук : 08.00.01 / А. А. Клочко. − М., 2001. − 205 с.

128. Коваль З. В. Політико-правові механізми державного управління інформаційно-психологічною безпекою України: дис. ... канд. наук з держ. упр. : 25.00.02 / З. В. Коваль. − Одеса, 2011. − 256 с.

129. Козубський В. О. Інформаційна безпека держави: Кримський регіон: автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.02 «Політичні інститути та процеси» / В. О. Козубський. − Сімферополь, 2005. − 19 с.

130. Козюбра М. І. Наукознавчі проблеми загальної теорії держави і права / М. І. Козюбра // Методологічні проблеми правової науки. − Х. : Право, 2003. − С. 91−94.

131. Козюбра Н. И. Понятие и структура методологии юридической науки / Н. И. Козюбра // Методологические проблемы юридической науки. − К. : Наук. думка, 1990. − С. 5−19.

132. Колесов О. Ю. Технологии функционального обеспечения систем информационной безопасности в политике: оценка отечественного и зарубежного опыта : оценка отечественного и зарубежного опыта : дис. ... канд. полит. наук : 23.00.02 / О. Ю. Колесов. − Н. Новгород, 2006. − 206 с.

133. Колісник А. С. Цивільно-правовий захист комп'ютерного програмного забезпечення : дис. ... канд. юрид. наук : 12.00.03 / А. С. Колісник. − О., 2007. − 187 с.

134. Колодій А. М. Громадянське суспільство та правова держава: шляхи розбудови / А. М. Колодій // Проблеми розбудови держави та громадянського суспільства в Україні : матер. наук.-прак. конф., 16-17 квіт. 2010 р., Київ / [відп. ред. Л. В. Кравченко]. − К. : Київ. нац. ун-т внутр. справ, 2010. − Ч. 1. − С. 20−24.

135. Колпаков В. К. Деліктний феномен в адміністративному праві України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / В. К. Колпаков. − К., 2005. − 37 с.

136. Конах В. К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад

США) : дис. ... канд. політ. наук : 21.01.01 / В. К. Конах. − К., 2005. − 171 с.

137. Конах В. К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США) : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 21.01.01 «Основи національної безпеки держави» / В. К. Конах. − К., 2005. − 20 с.

138. Конвенція про кіберзлочинність : Міжнародний документ від 23.11.2001 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

139. Корельский В. М. Теоретические проблемы социалистической государственной власти и демократии : дис. ... докт. юрид. наук : 12.00.01 / В. М. Корельский. − Свердловск, 1972. − 383 с.

140. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Б. А. Кормич. − Х., 2004. − 42 с.

141. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія / Б. А. Кормич. − О. : Юридична література, 2003. − 472 с.

142. Костецька Т. А. Право на інформацію в Україні / Т. А. Костецька. − К. : Вид-во «Вища школа», 1998. − 39 с.

143. Костицький М. Необхідність трансформації юридичної методології як бази розвитку права / М. Костицький // Український правовий часопис. − 2004. − №7. − С. 16−17.

144. Кохановська О. В. Цивільно-правові проблеми інформаційних відносин в Україні : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / О. В. Кохановська. − К., 2006. − 34 с.

145. Кохановська О. В. Теоретичні проблеми інформаційних відносин у цивільному праві / О. В. Кохановська. − К. : ВПЦ «Київський університет», 2006. − 463 с.

146. Кравчук М. В. Теорія держави і права / М. В. Кравчук. − К. : Атіка, 2003.− 140 с.

147. Красіков Д. О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України : дис. ... канд. юрид. наук : 12.00.07 / Д. О. Красіков. − К., 2012. − 220 с.

148. Красненкова Е. В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами : дис. ... канд. юрид. наук : 12.00.08 / Е. В. Красненкова. − М., 2006. − 188 с.

149. Красноступ Г. М. Організаційні та правові засади регулювання суспільних відносин щодо комп'ютерних програм : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Г. М. Красноступ. − Ірпінь, 2009. − 19 с.

150. Красноступ Г. М. Організаційно-правові аспекти необхідності реформування сучасного інформаційного законодавства [Електронний ресурс] : Міністерство юстиції України / Г. М. Красноступ. − Режим доступу : http://www.minjust.gov.ua /0/5461

151. Кретова Е. А. К вопросу об информации как объекте публичного права / Е. А. Кретова // Право и политика. − 2007. − № 11. − С. 107−109.

152. Кудря В. С. Функции правового государства, находящегося в становлении (на примере Российской Федерации) : дис. ... канд. юрид. наук : 12.00.01 / В. С. Кудря − М., 2005. − 190 с.

153. Кузенко Л. В. Правове регулювання права громадян на інформацію в сфері державного управління : дис. … канд. юрид. наук : 12.00.07 / Л. В. Кузенко − Х., 2003. − 173 с.

154. Куляница А. И. Парадигмы информациологической безопасности цивилизации / А. И. Куляница, О. В. Коломиец // Проблеми міжнародних відносин : зб. наук. праць / [наук. ред. Б. Канцелярук та ін.]. − К. : КиМУ, 2011. − Вип. 2. − С. 127−140.

155. Купцова О. Б. Экономическая функция Российского государства : дис. … канд. юрид. наук : 12.00.01 / О. Б. Купцова. − Н. Новгород, 2002. − 207 с.

156. Левин А. А. Приоритетные направления деятельности государства по обеспечению информационной безопасности

Российской Федерации (Политологический анализ) : дис. ... канд. полит. наук : 20.01.02 / А. А. Левин. − М., 2004. − 150 с.

157. Левицька М. Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України : дис. … канд. юрид. наук : 12.00.01 / М. Б. Левицька − К., 2002. − 206 с.

158. Левчук-Хмара М. В. Право в сучасному етико-філософському дискурсі : автореф. дис. на здобуття наук. ступеня канд. філософ. наук : спец. 09.00.07 «Етика» / М. В. Левчук-Хмара. − К., 2010. − 15 с.

159. Лемак В. В. Правова реформа в Чехії і Словаччині в умовах постсоціалістичної модернізації: теоретичні і практичні проблеми : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / В. В. Лемак. − Х., 2003. − 40 с.

160. Лившиц Р. З. Теория права : учеб. / Р. З. Лившиц. − 2-е изд. − М. : Издательство БЕК, 2001. − 224 с.

161. Ліпкан В. А. Національна безпека України : навч. посіб. / В.А. Ліпкан. − 2-е вид. − К. : КНТ, 2009. − 576 с.

162. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. − К. : КНТ, 2006. − 280 с.

163. Ліпкан В. А. Систематизація інформаційного законодавства України : монографія / В. А. Ліпкан, В. А. Залізняк; за заг. ред. В. А. Ліпкана. − К. : ФОП О. С. Ліпкан, 2012. − 304 с.

164. Ліпкан В. А. Теоретичні основи та елементи національної безпеки : монографія / В. А. Ліпкан. − К. : «Текст», 2003. − 600 с.

165. Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О. В. Логінов. − К., 2005. − 20 с.

166. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство. / В. Н. Лопатин. − М., 2000. − 428 с. – (Серия: Безопасность человека и общества).

167. Лопатин В. Н. Информационная безопасность России : дис. ... докт. юрид. наук : 12.00.01 / В. Н. Лопатин. − СПб., 2000. − 433 с.

168. Лощихін О. М. Теоретико-правові характеристики економічної функції сучасної держави : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / О. М. Лощихін. − К., 2010. − 32 с.

169. Лукич Р. Методология права / Р. Лукич. − М. : Прогресс, 1981. − 304 с.

170. Луць Л. А. Методологія порівняльного правознавства / Л.А. Луць // Проблеми державотворення і захисту прав людини в Україні : матеріали ІІІ регіон. наук. конф. − Л., 1997. − С. 29−34.

171. Луць Л. А. Загальна теорія держави і права : навч.-метод. посіб. (за кредитно-модульною системою) / Л. А. Луць. − К. : Атіка, 2007. − 412 с.

172. Мазаева Е. С. Социальная функция современного Российского государства : дис. ... канд. юрид. наук : 12.00.01 / Е. С. Мазаева. − Н. Новгород, 2001. − 160 с.

173. Макаренко Є. А. Міжнародна інформаційна політика: структура, тенденції, перспективи : дис. … докт. політ. наук: 23.00.04 / Є. А. Макаренко. − К., 2003. − 475 с.

174. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : дис. … канд. юрид. наук : 12.00.01 / Ю. Є. Максименко. − К., 2007. − 186 с.

175. Малько А. В. Теория государства и права в вопросах и ответах : учеб.-метод. пособие / А. В. Малько. − 4-е изд. перераб. и доп. − М. : Юристъ, 2004. − 300 с.

176. Мартиросян Т. А. Правовое обеспечение информационной безопасности Российской Федерации : дис. ... канд. юрид. наук : 12.00.14 / Т. А. Мартиросян. − М., 2005. − 210 с.

177. Маруженко О. П. Інформаційне забезпечення законотворчого процесу в Україні : дис. ... канд. юрид. наук : 12.00.07 / О. П. Маруженко. − К., 2009. − 202 с.

178. Марущак А. І. Правомірні засоби доступу громадян до інформації : науково-практичний посібник / А. І. Марущак. − Біла Церква : Вид-во «Буква», 2006. − 432 с.

179. Марущак А. І. Інформаційна безпека як об'єкт дослідження правової науки / А. І. Марущак // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-прак. конф., 17 березня 2010 року м. Київ. − К. : Наук. вид. відділ НА СБ України, 2010. − С. 36−41.

180. Марценюк О. Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О. Г. Марценюк. − К., 2009. − 20 с.

181. Мелихова А. В. Функции Советского и современного российского государства : дис. ... канд. юрид. наук : 12.00.01 / А. В. Мелихова. − Самара, 2006. − 246 с.

182. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О. О. Тихомиров, О. С. Лєнков // Збірник наукових праць Військового інституту Київського національного університету ім. Т .Г. Шевченка. – 2011. – Вип. 30. – С. 165–171.

183. Миндалёв И. В. Системы классификации [Електронний ресурс] : Теория экономических информационных систем : электрон. учеб.-метод. комплекс / И. В. Миндалёв. − Режим доступу : http://www.kgau.ru/istiki/teis/index.html

184. Миронов В. С. Экологическая функция государства: понятие, содержание, формы и методы осуществления (сравнительный анализ на примере России и Германии) : дис. ... канд. юрид. наук : 12.00.01 / В. С. Миронов. − Ростов-на-Дону, 2007. − 169 с.

185. Міжнародна поліцейська енциклопедія : у 10 т. Т. 1. Теоретико-методологічні та концептуальні засади поліцейського права та поліцейської деонтології / [відп. ред. Ю. І. Римаренко, Я. Ю. Кондратьєв, В. Я. Тацій, Ю. С. Шемшученко]. − К. : Концерн «Видавничій Дім «Ін Юре», 2003. − 1232 с.

186. Модельный информационный кодекс для государств-участников СНГ : Міжнародний документ від 03.04.2008 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

187. Морозов О. Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності [Електронний ре-

сурс] : Віче / О. Л. Морозов. − Режим доступу : http://www.viche.info/journal/598/

188. Морозова Л. А. Современная российская государственность (Проблемы теории и практики) : дис. ... докт. юрид. наук : 12.00.01 / Л. А. Морозова. − М., 1998. − 313 с.

189. Мотиль І. І. Становлення та розвиток внутрішніх функцій української держави : дис. … канд. юрид. наук : 12.00.01 / І. І. Мотиль. − К., 2007. − 214 с.

190.Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / О. І. Мотлях. − К., 2005. − 20 с.

191. Мухаев Р. Т. Теория государства и права : учеб. для вузов / Р. Т. Мухаев. − М. : «Издательство ПРИОР», 2002. − 364 с.

192. Надыгина Е. В. Теоретико-правовой анализ влияния информационных технологий на правосознание : дис. ... канд. юрид. наук : 12.00.01 / Е. В. Надыгина. − Н. Новгород, 2007. − 211 с.

193. Назаренко Г. В. Теория государства и права : учеб. пособие / Г. В. Назаренко. − М. : Издательство «Ось-89», 1999. − 159 с.

194. Настюк В. Я. Формування системи інформаційного законодавства в Україні / В. Я. Настюк // Інформація і право. − 2011. − № 2 (2). − С. 27−31.

195. Недбай В. Електронний уряд : теорія і практика [Електронний ресурс] / В. Недбай. − Режим доступу : http://bibl.kma.mk.ua/pdf/pidruchnuku/21/33.pdf

196. Недбайло П. Е. Введение в общую теорию государства и права (Предмет, система и функции науки) / П. Е. Недбайло. − К. : Изд-во «Вища школа», 1971. − 160 с.

197.Некляев С. Э. Участие средств массовой информации в обеспечении информационно-психологической безопасности в условиях локальных войн и международного терроризма : дис. ... канд. филол. наук : 10.01.10 / С. Э. Некляев. − М., 2003. − 149 с.

198. Нерсесянц В. С. Общая теория права и государства : учеб. для юрид. вузов и ф-тов / В. С. Нерсесянц. − М. : Издательство НОРМА, 2000. − 552 с.

199. Нижник Н. Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навч. посіб. / Н. Р. Нижник, Г. П. Ситник, В. Т. Білоус ; [заг. ред. П. В. Мельник, Н. Р. Нижник]. − Ірпінь, 2000. − 304 с.

200. Никодимов И. Ю. Информационно-коммуникативная функция государства и механизм ее реализации в современной России (Теоретический и сравнительно-правовой анализ) : дис. ... доктора юрид. наук : 12.00.01 / И. Ю. Никодимов − СПб., 2001. − 409 с.

201. Николаев А. А. Информационная безопасность России в условиях социальной трансформации (политологический анализ) : дис. ... канд. полит. наук : 23.00.02 / А. А. Николаев. − М., 2007. − 172 с.

202. Новая постидустриальная волна на Западе : антология / [под ред. В. Л. Иноземцева]. − М. : Academia, 1999. − 640 с.

203.Новиков Д. С. Участие в обеспечении мирового порядка как функция Российского государства : дис. ... канд. юрид. наук : 12.00.01 / Д. С. Новиков. − Владимир, 2005. − 190 с.

204. Новицька Н. Б. Організаційно-правові аспекти інформаційної культури в управлінській діяльності : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Н. Б. Новицька. − Ірпінь, 2007. − 19 с.

205. О типовых проектах законодательных актов МПА ЕврАзЭС в сфере информационных технологий («Об информатизации», «Об информационной безопасности», «Основные принципы электронной торговли») : Постановление Межпарламентской Ассамблеи Евразийского экономического сообщества от 28 мая 2004 г. № 5-20 [Електронний ресурс]. − Режим доступу : http://www.lawbelarus.com/world/sub01/texa0732.htm

206. Оборотов Ю. Н. Современное государство: основы теории : учеб. курс / Ю. Н. Оборотов. − О. : «Астропринт», 1998. − 260 с.

207. Окінавська хартія глобального інформаційного суспільства : Міжнародний документ від 22.07.2000 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

208. Оксамытный В. В. Теория государства и права : учебник для студ. высших учеб. заведений / В. В. Оксамытный. − М. : Изд-во «ИМПЭ-ПАБЛИШ», 2004. − 563 с.

209. Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О. В. Олійник. − К., 2006. − 20 с.

210. Оніщенко Н. М. Правова система: проблеми теорії : монографія / Н. М. Оніщенко. − К. : Ін-т держави і права ім. В. М. Корецького НАН України, 2002. − 352 с.

211. Оніщенко Н. М. Теоретико-методологічні засади формування та розвитку правової системи : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / Н. М. Оніщенко. − К., 2002. − 32 с.

212. Оніщенко Н. М. Розвиток соціальності сучасних державних і правових систем / Н. М. Оніщенко // Держава і право : зб. наук. пр. Юридичні і політичні науки. − К. : Ін-т держави і права ім. В. М. Корецького НАН України, 2001. − Вип. 14. − С. 3−11.

213. Оніщенко Н. М. Сприйняття права в умовах демократичного розвитку: проблеми, реалії, перспективи : монографія / Н. М. Оніщенко / [відп. ред. Ю. С. Шемшученко]. − К. : ТОВ «Видавництво «Юридична думка», 2008. − 320 с.

214. Онопенко П. В. Правоохоронні функції держави Україна / П. В. Онопенко. − К. : «Варта», 2003. − 128 с.

215. Орлов С. О. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» / С. О. Орлов. − Х., 2004. − 20 с.

216. Основи інформаційного права України : навч. посіб. / В. С. Цимбалюк, В. Д. Гавловський та ін. ; [ред. М. Я. Швець, Р. А. Калюжний, П. В. Мельник]. − К. : Знання, 2004. − 274 с.

217. Основные события ШОС в 2007 году [Електронний ресурс] : Шанхайская организации сотрудничества. − Режим доступу : http://www.sectsco.org/RU/show.asp?id=11

218. Остроухов В. В. Соціально-правові основи інформаційної безпеки : навч. посіб. / В. В. Остроухов, В. М. Петрик, А. М. Кузьменко та ін. ; [ред. В. В. Остроухов]. − К. : Росава, 2007. − 495 с.

219. Оськина Е. А. Функции государства по обеспечению экономической безопасности России : дис. ... канд. экон. наук : 08.00.01 / Е. А. Оськина. − Саратов, 2006. − 177 с.

220. Оценка прогресса, достигнутого в осуществлении решений и последующей деятельности по итогам Всемирной встречи на высшем уровне по вопросам информационного общества : Резолюция Экономического и Социального Совета № 2010/2 от 19 июля 2010 года [Електронний ресурс]. − Режим доступу : http://www.un.org/ru/ecosoc/docs/2010/r2010-2.pdf

221. Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / Л. П. Паламарчук. − К., 2005. − 18 с.

222. Панарин А. С. Глобальное информационное общество: вызовы и ответы / А. С. Панарин // Глобальная информатизация и безопасность России / [общ. ред. В. И. Дебреньков]. − М. : Изд-во Московского университета, 2001. − 398 с.

223. Панарин И. Н. Информационная война и геополитика / И. Н. Панарин. − М. : Изд-во «Поколение», 2006. − 560 с.

224. Панкевич О. З. Соціальна держава: поняття та загальнотеоретична характеристика : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / О. З. Панкевич. − Л., 2003. − 20 с.

225. Панченко В. М. Гуманітарна та технологічна складові у визначенні поняття «інформаційна безпека» / В. М. Панченко // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-прак. конф., 17 березня 2010 року, м. Київ. − К. : Наук.-вид. відділ НА СБ України, 2010. − С. 205−206.

226. Панченко В. М. Методика виявлення ознак інформаційного впливу в засобах масової інформації / В. М. Панченко, В. І. Полевий // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3 (7). – С. 70–77.

227. Панченко В. М. Структурно-функціональний аналіз загальнодержавної системи забезпечення інформаційної безпеки / В. М. Панченко // Інформаційна безпека людини, суспільства, держави : наук.-практ. журн. − 2009. − № 1 (1). − С. 48−51.

228. Пастухов О. М. Авторське право у сфері функціонування всесвітньої інформаційної мережі Інтернет : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / О. М. Пастухов. − К., 2002. − 18 с.

229. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / Д. В. Пашнєв. − Х., 2007. − 18 с.

230. Пеньков И. А. Обеспечение информационной безопасности Российской Федерации в глобальной сети Интернет (Политологический анализ) : дис. ... канд. полит. наук : 23.00.02 / И. А. Пеньков. − М., 2005. − 153 с.

231. Петкова О. В. Політичні імперативи позиціонування України в міжнародному інформаційному просторі : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.04 «Політичні проблеми міжнародних систем та глобального розвитку» / О. В. Петкова. − К., 2010. − 20 с.

232. Пилипчук В. Г. Проблеми становлення і розвитку інформаційного законодавства в контексті євроінтеграції України / В. Г. Пилипчук, В. М. Брижко // Інформація і право. − 2011. − № 1 (1). − С. 11−19.

233. Письменицкий А. А. Информационное право Украины / А. А. Письменицкий. − Х. : «Бизнес Информ», 1996. − 208 с.

234. Питання концепції реформування інформаційного законодавства України / [Р. А. Калюжний, В. С. Цимбалюк, В. Д. Гавловський, М. В. Гуцалюк] // Правове, нормативне та

метрологічне забезпечення захисту інформації в Україні. − К. : НТУУ «КПІ», 2000. − С. 17−21.

235. Пожарский Д. В. Контрольно-надзорная функция современного государства : дис. ... канд. юрид. наук : 12.00.01 / Д. В. Пожарский − М., 2004. − 222 с.

236. Полевий В. І. Система забезпечення інформаційної безпеки України в контексті системності інформаційних загроз / В. І. Полевий // Наук. вісн. НА СБ України. − 2006. − №24. − С. 153−162.

237. Поливанюк В. Д. Особливості розслідування злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / В. Д. Поливанюк. − К., 2008. − 17 с.

238. Поляков А. В. Общая теория права: Проблемы интерпретации в контексте коммуникативного подхода / А. В. Поляков. − СПб. : Издательский Дом Санкт-Петербургского гос. ун-та, 2004. − 864 с.

239. Полякова Т. А. Теоретико-правовой анализ законодательства в области обеспечения информационной безопасности Российской Федерации : автореф. дис. … канд. юрид. наук. : 12.00.01 / Т. А. Полякова. − М., 2002. − 24 с.

240. Полякова Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России : автореф. дис. … докт. юрид. наук. : 12.00.14 / Т. А. Полякова. − М., 2008. − 38 с.

241. Порядок надання інформаційних та інших послуг з використанням електронної інформаційної системи «Електронний Уряд», затверджений Наказом Державного комітету зв’язку та інформатизації України № 149 від 15.08.2003 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

242. Постанова Кабінету Міністрів України «Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи (словник термінів)» № 40 від 20.01.1997 (втратила чинність) [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

243. Почуев С. Internet и информационная безопасность России [Електронний ресурс] : SciTecLibrary.ru / С. Почуев. − Режим доступу : http://www.sciteclibrary.ru/rus/catalog/pages /854.html

244. Правове забезпечення інформаційної діяльності в Україні / [заг. ред. Ю. С. Шемшученко, І. С. Чиж]. − К. : ТОВ «Видавництво «Юридична думка», 2006. − 384 с.

245. Правове регулювання інформаційної діяльності в Україні / [упоряд. С. Е. Демський]. − К. : Юрінком Інтер, 2001. − 688 с.

246. Про державну таємницю : Закон України №3855-XII від 21.01.1994 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

247. Про Доктрину інформаційної безпеки України : Указ Президента України №514/2009 від 08.07.2009 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua.

248. Про доступ до публічної інформації : Закон України №2939-VI від 13.01.2011 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

249.Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра : Постанова Кабінету Міністрів України №787 від 27.08.2010 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

250. Про інформацію : Закон України №2657-XII від 02.10.1992 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

251.Про Концепцію національної інформаційної політики : проект Закону України №2526 від 13.12.2002 [Електронний ресурс]. − Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb_n /webproc4_2?id=&pf3516=2526&skl=5

252. Про Концепцію Національної програми інформатизації : Закон України №75/98-ВР від 04.02.1998 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

253. Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України : Постанова Правління Національного банку України №474 від

28.10.2010 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

254. Про Основи національної безпеки : Закон України №964-IV від 19.06.2003 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

255. Про Основні засади розвитку інформаційного суспільства в Україні на 2007−2015 роки : Закон України №537-V від 09.01.2007 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

256. Про телекомунікації : Закон України №1280-IV від 18.11.2003 [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua

257. Проблеми і пріоритети розвитку правової науки в інформаційній сфері (Рекомендації «круглого столу») // Інформація і право. − № 1 (1). − 2011. − С. 8−10.

258. Программа ЮНЕСКО «Информация для всех» 17-24 августа 2001, Бостон, США [Електронний ресурс]. − Режим доступу : http://www.nbuv.gov.ua/law/00_uiv.html#3

259. Проект закону України «Про Національну програму «Україна-2010» №3187 від 13.04.1999 року [Електронний ресурс]. − Режим доступу: http://gska2.rada.gov.ua/pls/zweb_n/webproc34?id=&pf3511=5837&pf35401=591

260. Проект Федерального Закона «Об информационно-психологической безопасности» [Електронний ресурс]. − Режим доступу : http://www.medialaw.ru/publications/zip/68/lopatin.htm

261. Прокоф'єва Д. Інформація як предмет злочину [Електронний ресурс] : Центр информационной безопасности / Д. Прокоф'єва. − Режим доступу : http://www.bezpeka.com/ru/lib/spec/law/information-as-the-subject-of-crime.html

262. Протасов В. Н. Теория права и государства. Проблемы теории права и государства: вопросы и ответы / В. Н. Протасов. − М. : Новый юрист, 1999. − 268 с.

263. Пушкин А. И. Образовательная функция современного Российского государства : дис. ... канд. юрид. наук : 12.00.01 / А. И. Пушкин. − Н. Новгород, 2002. − 195 с.

264. Рабінович П. М. Основи загальної теорії права та держави : посіб. для студ. спец. «Правознавство».

/П. М. Рабінович. − 2-е вид. зі змін. і доп. − К. : Навчальне видання, 1994. − 238 с.

265. Рабінович П. М. Основи загальної теорії права та держави : навч. посіб. / П. М. Рабінович. − 6-е вид. − Х. : Консум, 2002. − 141 с.

266. Рабінович П. М. Трансформація методології вітчизняного праводержавознавства: досягнення і проблеми / П. М. Рабінович // Юридична Україна. − 2003. − №1. − С. 20−25.

267. Расторгуев С. П. Информационная война / С. П. Расторгуев. − М. : Радио и связь, 1999. − 416 с.

268. Расторгуев С. П. Выборы во власть как форма информационной экспансии / С. П. Расторгуев. − М. : Новый век, 1999. − 27 с.

269. Рекомендації міжнародної науково-теоретичної конференції «Проблеми методології сучасного правознавства» // Вісник Академії правових наук. − 1997. − №1(8). − С. 150−154.

270. Ровинская Т. Л. Информационная глобализация: вызов культурной самобытности европейских государств / Т. Л. Ровинская // Государство в эпоху глобализации: экономика, политика, безопасность / [отв. ред. Ф. Г. Войтоловский и А. В. Кузнецов]. − М. : ИМЭМО РАН, 2008. − Вып. 3 : Мировое развитие. − 219 с.

271. Родионова О. В. Социальная функция современного государства : дис. ... докт. юрид. наук : 12.00.01 / О. В. Родионова. − М., 2007. − 353 с.

272. Розенфельд Н. А. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» / Н. А. Розенфельд. − К., 2003. − 17 с.

273. Рудик М. В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» / М. В. Рудик. − О., 2007. − 19 с.

274. Рымарева Н. В. Концептуальные вопросы формирования системы правового регулирования информационной безопасности в Российской Федерации : дис. ... канд. юрид. наук : 05.13.19 / Н. В. Рымарева. − Воронеж, 2005. − 182 с.

275. Сагатовский В. Н. Системная деятельность и ее философское осмысление / В. Н. Сагатовский // Системные исследования. Методологические проблемы : ежегодник, 1980. − М. : Наука, 1981. − С. 52−68.

276. Садовничий В. А. Информационная безопасность: новые угрозы мировому сообществу / В. А. Садовничий // Глобальная информатизация и безопасность России / [общ. ред. В. И. Дебреньков]. − М. : Изд-во Московского гос. ун-та, 2001. − 398 с.

277. Сало В. І. Внутрішні функції держави в умовах членства в Європейському Союзі : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / В. І. Сало. − Х., 2008. − 22 с.

278. Сало В. І. Поняття, ознаки та класифікація функцій держави [Електронний ресурс] / В. І. Сало // Державне будівництво та місцеве самоврядування. − 2009. − Вип. 17. − Режим доступу : http://www.nbuv.gov.ua/portal/Soc_Gum/Dbms/2009_17/Salo.pdf

279.Самбиев А. Технический анализ социальных систем [Електронний ресурс] / А. Самбиев. − Режим доступу : http://lib.kharkov.ua/POLITOLOG/sambiev.txt_with-big-pictures.html

280. Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп’ютерних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / О. А. Самойленко. − Х., 2007. − 20 с.

281. Самойленко В. А. Социальная функция современного российского государства : дис. ... канд. юрид. наук : 12.00.01 / В. А. Самойленко. − Коломна, 2006. − 220 с.

282. Селіванов М. В. Захист права на комп’ютерну програму (авторсько-правовий аспект) : автореф. дис. на здобуття

наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / М. В. Селіванов. − Х., 2002. − 20 с.

283. Сердюк О. В. Соціологічний підхід у сучасному правознавстві: філософсько-правове дослідження : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.12 «Філософія права» / О. В. Сердюк. − Х., 2010. − 40 с.

284. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. / В. С. Сідак, В. Ю. Артемов. − К. : КНТ, 2007. − 160 с.

285. Скакун О. Ф. Теория государства и права : учеб. / О. Ф. Скакун. − Х. : Консум, 2000. − 245 с.

286. Солодка О. М. Забезпечення інформаційної безпеки у процесі євроатлантичної інтеграції України / О. М. Солодка // Інформаційна безпека особи, суспільства, держави : наук.-практ. журн. − 2009. − №1(1). − С. 52−56.

287. Солоненко О. М. Реалізація функції забезпечення законності, правопорядку, охорони прав, свобод і законних інтересів громадян у системі місцевого самоврядування (організаційно-правові питання) : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.02 «Конституційне право; муніципальне право» / О. М. Солоненко. − К., 2001. − 19 с.

288. Сопілко І. М. До питання класифікації інформації / І. М. Сопілко // Становлення держави та права в умовах глобалізації: теоретичний та практичний аспект : матеріали II Міжнар. наук. конф. (Київ, НАУ, 24 лютого 2012 р.). – Ніжин : Видавець ПП Лисенко М. М., 2012. – С. 161−163.

289. Сопілко І. М. Правове регулювання відносин щодо отримання органами державної влади України інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / І. М. Сопілко. − К., 2010. − 20 с.

290. Сорокин Д. В. Проблемы правового обеспечения информационной безопасности России в условиях глобализации информационного пространства : дис. ... канд. юрид. наук : 12.00.14 / Д. В. Сорокин. − СПб., 2006. − 223 с.

291. Соснін О. Проблеми правового регулювання інформаційної політики в Україні [Електронний ресурс] : Віче / О. Соснін. − Режим доступу : http://www.viche.info /journal/1159/

292. Спиридонов Л. И. Теория государства и права / Л. И. Спиридонов. − М., 2001. − 304 с.

293. Статистика МВС: Стан та структура злочинності в Україні [Електронний ресурс]. − Режим доступу : http://www.mvs.gov.ua

294. Стратегический план ПИДВ на 2008-2013 гг. IFAP-2008/COUNCIL.V/4 Париж, февраль 2008 г. [Електронний ресурс]. − Режим доступу : http://www.ifap.ru/pr/2008/n080331a.pdf

295. Стрельбицька Л. М. Державне управління крізь призму інформаційної безпеки України / Л. М. Стрельбицька, М. П. Стрельбицький // Інформаційна безпека особи, суспільства, держави : наук.-практ. журн. − 2009. − № 2 (2). − С. 53−56.

296. Стрельцов А. А. Теоретические и методологические основы правового обеспечения информационной безопасности России : дис. ... докт. юрид. наук : 05.13.19 / А. А. Стрельцов. − М., 2004. − 371 с.

297. Стрельцов А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы / А. А. Стрельцов ; [ред. В. А. Садовничий, В. П. Шерстюк]. − М. : МЦМНО, 2002. − 296 с.

298.Субіна Т. В. Адміністративно-правове забезпечення інформаційної безпеки в органах Державної податкової служби України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Т. В. Субіна. − Ірпінь, 2010. − 22 с.

299. Сугестивні технології маніпулятивного впливу : навч. посіб. / [заг. ред. Є.Д. Скулиш]. − К. : Наук. вид. відділ НА СБ України, 2010. − 248 с.

300.Судоргин О. А. Императивы и приоритеты политики обеспечения информационной безопасности России : дис. ... канд. полит. наук : 23.00.02 / О. А. Судоргин. − М., 2005. − 202 с.

301. Сулацький Д. В. Організаційно-правові засади забезпечення інформаційної безпеки людини як споживача телеко-

мунікаційних послуг : дис. ... канд. юрид. наук : 12.00.07 / Д. В. Сулацький. − Херсон, 2011. − 290 с.

302. Супрун В. М. Теоретико-правові основи інформаційного суверенітету : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень» / В. М. Супрун. − Х., 2010. − 20 с.

303.Сурилов А. В. Теория государства и права : учеб. пособие / А. В. Сурилов. − К. : Изд-во «Выща школа», 1989. − 439 с.

304. Сучасний тлумачний словник української мови : 65000 слів / [заг. ред. В. В. Дубчинський]. − Х. : ВД «ШКОЛА», 2006. − 1008 с.

305. Тамодлин А. А. Государственно-правовой механизм обеспечения информационной безопасности личности : дис. ... канд. юрид. наук : 12.00.01 / А. А. Тамодлин. − Саратов, 2006. − 175 с.

306. Тарановский Ф. В. Учебник энциклопедии права / Ф. В. Тарановский. − Юрьев, 1917. − 537 с.

307. Тарановский Ф. В. Энциклопедия права / Ф. В. Тарановский. − 3-е изд. − СПб. : Изд-во «Лань», 2001. − 560 с.

308. Тарасов Н. Н. Метод и методологический подход в правоведении (попытка проблемного анализа) / Н. Н. Тарасов // Правоведение. − 2001. − №1. − С. 31−50.

309. Тацишин І. Б. Адміністративно-правове забезпечення інформаційних відносин в галузі реклами : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / І. Б. Тацишин. − Л., 2009. − 18 с.

310.Тененбаум В.Л. Государство: система категорий / В. Л. Тененбаум. − Саратов : Изд-во Сарат. ун-та, 1971. − 212 с.

311. Теория государства и права / [ред. В. М. Корельский, В. Д. Перевалов]. − М., 1997. − 570 с.

312. Теория государства и права : курс лекций / [ред. Н. И. Матузов, А. В. Малько]. − М., 1997. − 672 с.

313. Теорія держави і права : навч. посіб. / [заг. ред. В. В. Копєйчиков]. − К. : Юрінформ, 1995. − 192 с.

314. Теорія держави і права : підруч. / [С. Л. Лисенков (ред.), А. М. Колодій, О. Д. Тихомиров, В. С. Ковальський]. − К. : Юрінком Інтер, 2005. − 448 с.

315. Терехин Д. В. Охрана международного правопорядка как функция современного Российского государства : дис. ... канд. юрид. наук : 12.00.01 / Д. В. Терехин. − Н. Новгород, 2006. − 266 с.

316. Тимошин С. К. Трансформация функций государства в условиях глобализации : дис. ... канд. экон. наук : 08.00.01 / С. К. Тимошин. − Саратов, 2006. − 154 с.

317. Тихомиров А. Д. Юридическая компаративистика: философские, теоретические и методологические проблемы / А. Д. Тихомиров. − К. : Знання, 2005. − 334 с.

318. Тихомиров О. О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: мета, засоби і методи, принципи, результати / О.О. Тихомиров // Інформаційна безпека людини, суспільства, держави. – 2012. – № 3 (10). – С. 11–17.

319. Тихомиров О. О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: об’єкти і суб’єкти / О. О. Тихомиров // Інформаційна безпека людини, суспільства, держави. – 2012. – № 2 (9). – С. 18–24.

320. Тихомиров О. О. До проблеми розуміння функцій сучасної держави / О. О. Тихомиров // Підприємництво, господарство і право. − 2009. − № 1. − С. 72−75.

321. Тихомиров О. О. Забезпечення інформаційної безпеки: теоретико-правовий аспект / О. О. Тихомиров // Право України. − 2011. − № 4. − С. 252−259.

322. Тихомиров О. О. Класифікації забезпечення інформаційної безпеки / О. О. Тихомиров // Вісник Запорізького національного університету : зб. наук. праць. Юридичні науки. − Запоріжжя : Запорізький національний університет. − 2011. − №1. − С. 164−169.

323. Тихомиров О. О. Критеріальна оцінка інформаційного розвитку суспільства та інформаційної безпеки / О. О. Тихомиров / Бюлетень Міністерства юстиції України. − 2010. − № 4−5. − С. 250−254.

324. Тихомиров О. О. Критеріальний метод у правових дослідженнях / О. О. Тихомиров // Філософські, методологічні і психологічні проблеми права : тези доп. ІІІ Всеукр. наук.-практ.

конф. (Київ 23 квітня 2010 р.) / [редкол. : В. В. Коваленко, М. В. Костицький, О. М. Джужа та ін.] − К. : Київ. нац. ун-т внутр. справ, 2010. − С. 206−207.

325. Тихомиров О. О. Перспективні зміни поняття інформаційної безпеки / О. О. Тихомиров // Правова інформатика. − 2010. − № 4 (28). − С. 68−75.

326. Тихомиров О. О. Правова інформація: теоретико-правовий аспект / О.О. Тихомиров // Інформаційна безпека людини, суспільства, держави. – 2012. – № 1 (8). – С. 29–35.

327. Тодика Ю. М. Тлумачення Конституції і законів України: теорія та практика : монографія / Ю. М. Тодика. − Х. : Факт. 2003. − 322 с.

328. Токарська А. С. Правова комунікація в контексті посткласичного праворозуміння : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.12 «Філософія права» / А. С. Токарська. − К., 2008. − 35 с.

329. Тоффлер Э. Создание новой цивилизации. Политика третьей волны [Електронний ресурс] / Э. Тоффлер, Х. Тоффлер. − Режим доступу : http://www.freenet.bishkek.su/jornal/n5 /JRNAL511.htm

330. Триняк В. Ю. Інформаційна безпека як соціокультурний феномен (соціально-філософський аналіз) : автореф. дис. на здобуття наук. ступеня канд. філософ. наук : спец. 09.00.03 «Соціальна філософія та філософія історії» / В. Ю. Триняк. − Д., 2009. − 19 с.

331. Троцький Я. О. Глобалізаційні виклики національній безпеці України в контексті європейських інтеграційних процесів : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 21.01.01 «Основи національної безпеки держави» / Я. О. Троцький. − К., 2010. − 20 с.

332. Философский энциклопедический словарь / [редкол. : С. С. Аверинцев, Э. А. Араб-Оглы, Л. Ф. Ильичев и др.] − 2-е изд. − М. : Сов. Энциклопедия, 1989. − 815 с.

333. Харченко Л. С. Інформаційна безпека України : глосарій / Л. С. Харченко, В. А. Ліпкан, О. В. Логінов ; [заг. ред. Р. А. Калюжний]. − К. : «Текст», 2004. − 134 с.

334. Хорошко В. О. Методика кількісно-якісного аналізу та визначення рівня інформаційної безпеки [Електронний ресурс] / В. О. Хорошко, В. С. Чередниченко // Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія». − Режим доступу : http://www.nbuv.gov.ua/portal/natural/Itki/2008_3/08hvafis.pdf

335. Хохлов И. И. Субсидиарность как принцип и механизм политики Европейского Союза [Електронний ресурс] : Национальная и государственная безопасность Российской Федерации / И. И. Хохлов. − Режим доступу : http: //www.nationalsecurity.ru/library/00018/index.htm

336. Храбан І. А. Конфігурація європейської безпеки в контексті реалізації національних інтересів України (воєнно-політичний аспект) : автореф. дис. на здобуття наук. ступеня докт. політ. наук : спец. 21.01.01 «Основи національної безпеки держави» / І. А. Храбан. − К., 2008. − 32 с.

337. Цимбалюк В. С. Інформаційне право (основи теорії і практики) : монографія / В. С. Цимбалюк − К. : «Освіта України», 2010. − 388 с.

338. Цыденова О. М. Философско-этические основания информационной безопасности : дис. ... канд. филос. наук : 09.00.11 / О. М. Цыденова. − Улан-Удэ, 2005. − 145 с.

339. Чернов А. Основные историко-теоретические этапы развития концепций глобального информационного общества [Електронний ресурс] / А. Чернов. − Режим доступу : http://www.isn.ru/public/is.doc

340. Черноголовкин Н. В. Теория функций социалистического государства / Н. В. Черноголовкин. − М. : Юридическая литература, 1970. − 216 с.

341. Шадрин А. Трансформация экономических и социально-политических институтов в условиях перехода к информационному обществу [Електронний ресурс] / А. Шадрин. − Режим доступу : http://www.ieie.nsc.ru/parinov/artem1.htm

342. Швець М. До питання систематизації інформаційного законодавства України / М. Швець, В. Брижко // Правова інформатика. − 2007. − № 4 (16). − С. 5−8.

343. Шершеневич Г. Ф. Общее учение о праве и государстве : лекции / Г. Ф. Шершеневич. − М. : Моск. об-во народ. унтов, 1911. − 163 с.

344. Шкарупа В.К. Застосування положень права щодо формування основ теорії інформаційного права / В. К. Шкарупа, В. С. Цимбалюк // Правова інформатика. − 2006. − № 3. − С. 44−51.

345. Шмелев А. А. О правовой информации [Електронний ресурс] : Научный центр правовой информации / А. А. Шмелев. − Режим доступу : http://www.scli.ru/rights/

346. Шрадер Х. Глобализация, (де)цивилизация и мораль [Електронний ресурс] / Х. Шрадер. − Режим доступу : http://www.soc.pu.ru:8101/publications /jssa/1998/2/6schrad.html

347. Штихве Р. К генезису мирового общества. Инновации и механизмы [Електронний ресурс] / Р. Штихве. − Режим доступу : http://www.soc.pu.ru:8101/publications/jssa/1999/3 /5stichw.html

348. Юридичний словник-довідник / [ред. Ю. С. Шемшученко]. − К. : Феміна, 1996. − 696 с.

349. Язык закона / [ред. А. С. Пиголкин]. − М. : Юридическая литература, 1990. − 192 с.

350. Янина Е. В. Гражданско-правовое регулирование информационной безопасности : дис. ... канд. юрид. наук : 12.00.03, 12.00.14 / Е. В. Янина. − М., 2004. − 166 с.

351. Яременко І. А. Комунікативне вчення Юргена Хабермаса в проблемному полі незавершеності модерну : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 09.00.05 «Історія філософії» / І. А. Яременко. − Д., 2007. − 17 с.

352. Action plan for a Safer Internet 1999-2004 [Електронний ресурс]. − Режим доступу : http://europa.eu /legislation_summaries/information_society/l24190_en.htm

353. Basic documents UNESCO 1989-1995/ News Communication Strategy. Document C II−96/WS/2. − Paris, UNESCO, 1995. − 109 p.

354. BSI и BS 7799 − Видение разработчиков [Електронний ресурс] : ISO27000.ru. − Режим доступу :

http://www.iso27000.ru/chitalnyi-zai/standarty-informacionnoi-bezopasnosti/bsi-i-bs-7799-2013-videnie-razrabotchikov

355. Building the European Information Society for Us All. First Reflections of the High Level Group of Experts. Interim Report. − Brussels, 1996

356. Cybercrime training for judges and prosecutors: a concept [Електронний ресурс]. − Режим доступу : http://www.coe.int/t/DGHL/cooperation/LisbonNetwork/meetings/Autre/2079_train_concept_4_provisional_8oct09_en.pdf

357.eEurope 2005 Executive summary [Електронний ресурс]. − Режим доступу : http://ec.europa.eu/information_society /eeurope/2002/news_library/documents/eeurope2005/execsum_en.pdf

358. eEurope 2005: An information society for all. An Action Plan to be presented in view of the Sevilla European Council, 21/22 June 2002 [Електронний ресурс]. − Режим доступу : http://ec.europa.eu/information_society/eeurope/2002/news_library /documents/eeurope2005/eeurope2005_en.pdf

359. Europe's Way to the Information Society: An Action Plan by the European Commission. − Brussels, 1994.

360. Green Paper. Living and Working in the Information Society: People First. European Comission. − Brussels, 1996.

361. ISO/IEC 27002:2005 Information technology. Security techniques. Code of practice for information security management [Електронний ресурс]. − Режим доступу : http://www.iso.org /iso/catalogue_detail?csnumber=50297

362. Lisbon European Council 23 and 24 march 2000. Presidency conclusions. [Електронний ресурс]. − Режим доступу : http://www.europarl.europa.eu/summits/lis1_en.htm

363. Networks for People and their Communities. Making the Most of the Information Society in European Union. − Brussels, 1996.

364. North Atlantic Council, summary Record of the Meeting of the Council on March 2, 1995 (Brussels: NATO Archives, March 2, 1995), C−R (55)8 [Електронний ресурс]. − Режим доступу : http://rr.sans.org/policy/sensitive.php

365. White Paper. The Challenges and Ways Forward into the 21st Century. − Brussels, 1993.

Наукове видання

Тихомиров Олександр Олександрович

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ФУНКЦІЯ СУЧАСНОЇ ДЕРЖАВИ

Монографія

Редактор *Н. М. Мармоленко*
Технічний редактор *О. С. Вишневська*

Формат 60х84/16. Ум. друк. арк. 11,16.
Обл.-вид. арк. 9,18. Тираж 300 пр. Зам. №

Видавець і виготовлювач
Центр навчально-наукових та науково-практичних видань
Національної академії Служби безпеки України,
вул. Трутенка, 22, м. Київ-22, 03022
Свідоцтво суб'єкта видавничої справи ДК № 99 від 23.06.2000