Інформаційна і національна безпека

УДК 340+35.078.3

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

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: ОНТОЛОГІЧНІ ВИМІРИ

Анотація. *У статті досліджується зміст категорії “система інформаційної безпеки” та визначаються складові відповідної системи, а також обґрунтовується необхідність розмежування системи інформаційної безпеки та системи забезпечення інформаційної безпеки.*

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

Summary. *The article explores the content of the category “information security system” and determines the components of this system, and also substantiates the need to delimit the information security system and the information security ensuring system.*

Keywords: *information security, information security ensuring, national security, system, state, process, threat.*

Аннотация. *В статье исследуется содержание категории “система информационной безопасности” и определяются составляющие соответствующей системы, а также обосновывается необходимость размежевания системы информационной безопасности и системы обеспечения информационной безопасности.*

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

Постановка проблеми. Постійне зростання ролі інформаційних ресурсів у житті сучасного суспільства та значення інформаційного впливу на суспільну свідомість внаслідок небаченого розширення медіа-поля, запровадження новітніх інформаційних технологій, удосконалення інформаційної інфраструктури зумовлює необхідність приділення дедалі більшої уваги проблемі інформаційної безпеки. Інформація стає сьогодні головним ресурсом науково-технічного й соціально-економічного розвитку суспільства, який, на відміну від переважної більшості традиційних ресурсів, не тільки не зменшується внаслідок використання, але й неухильно зростає, забезпечуючи зростання життєвого рівня населення, економічного, оборонного і політичного потенціалу країни. Цілісність світового співтовариства також забезпечується за рахунок інтенсивного інформаційного обміну. У цих умовах інформаційна сфера життєдіяльності суспільства стає дедалі більш уразливою мішенню для інформаційної агресії й тероризму, відтак кожна держава повинна забезпечити в країні відповідний рівень інформаційної безпеки як на національному рівні, так і на рівні організацій і окремих громадян. Системний характер впливу на інформаційну безпеку великої сукупності різнопланових факторів, що мають до того ж різну фізичну природу та переслідують різні цілі, а також викликають різні наслідки, призводить до необхідності комплексного підходу до вирішення цієї проблеми.

На сьогодні в Україні закладена основа правового регулювання забезпечення національної безпеки й інформаційної безпеки зокрема, завдяки чому одержали своє законодавче закріплення основні поняття в області національної безпеки, а також правове обґрунтування системи її забезпечення. Разом з тим, основні нормативно-правові акти у сфері інформаційної безпеки вимагають доопрацювання, зокрема, в аспекті визначення й законодавчого закріплення поняття й змісту категорії “система інформаційної безпеки”, а також розробки теоретичних і правових засад її забезпечення.

Результати аналізу наукових публікацій. Проблематика інформаційної безпеки та її забезпечення у різних аспектах досліджувались у наукових працях Х. Андерсена, О. Баранова, В. Брижка, Н. Влажика, В. Горбуліна, В. Гурковського, О. Дзьобаня, О. Довганя, Г. Ємельянова, Р. Калюжного, Б. Кормича, Дж. Кріка, В. Ліпкана, В. Лопатіна, Р. Максутова, А. Марущака, А. Нашинець-Наумової, М. Ніелса, В. Остроухова, М. Панова, В. Пилипчука, М. Потрубача, Г. Почепцова, М. Присяжнюка А. Прозорова, С. Расторгуєва, В. Рубана, С. Стрельцова, О. Тихомирова, М.-Дж. Шварца та інших вітчизняних та зарубіжних дослідників. Водночас, слід констатувати, що ні в сучасній науковій літературі, ні на законодавчому рівні поки не склалося єдиного підходу до розуміння системи інформаційної безпеки держави. На практиці це призводить не лише до активізації наукової дискусії, але й до неадекватності розуміння змісту тих або інших положень, висновків і рекомендацій, що стосуються сфери інформаційної безпеки України і мають прикладне значення. Зокрема, наразі немає єдиного підходу до визначення системи інформаційної безпеки як на доктринальному, так і на нормативному рівні, що свідчить про актуальність дослідження з відповідної проблематики.

Метою статті є визначення змісту категорії “система інформаційної безпеки” та складових відповідної системи.

Виклад основного матеріалу. Відповідно до ст. 17 Конституції України захист інформаційної безпеки, нарівні із захистом суверенітету та територіальної цілісності України, є найважливішою функцією держави та справою всього Українського народу [1], то ж інформаційна безпека, безперечно, є однією з найважливіших складових національної безпеки України. Оскільки інформаційна сфера має своїм змістом знання про інші сфери життєдіяльності суспільства, вона одночасно існує як самостійно, так і у взаємозв’язку з іншими сферами життєдіяльності суспільства, оскільки здійснює їх “інформаційне обслуговування” за допомогою інформації. Це зумовлює виняткове значення інформаційної сфери та загроз, що на неї спрямовані, адже, як справедливо зазначає Г. Сащук, “…під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав’язуються чужі інтереси, мотиви, спосіб життя” [2], а на думку В. Ліпкана “національні інтереси, загрози їм, управління цими загрозами в усіх галузях національної безпеки знаходять свій вираз, реалізуються через інформацію та інформаційну сферу” [3]. Відтак забезпечення інформаційної безпеки є запорукою забезпечення інших складових національної безпеки, адже всі типи взаємовідносин між суб’єктами інформаційного суспільства ґрунтуються на споживанні й обміні інформацією, а когнітивний простір багато в чому не лише обслуговує й супроводжує, але й підміняє реальний.

Досліджуючи питання системи інформаційної безпеки, передусім слід визначитись із тим, що саме ми розуміємо під інформаційною безпекою, адже наразі з цього приводу наука досі не має єдиної думки. Зокрема, О. Данільян, О. Дзьобань та М. Панов визначають інформаційну безпеку як безпеку об’єкта від інформаційних загроз або негативних впливів, пов’язаних з інформацією, та нерозголошення даних про той чи інший об’єкт, що є державною таємницею [4]. В. Гурковський вважає, що інформаційна

безпека – це суспільні відносини, пов’язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [5]. Інша група вчених [6] під інформаційною безпекою розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни.

В. Ярочкін та Т. Шевцова зазначають, що інформаційна безпека – це проведення правових, організаційних та інженерно-технічних заходів при формуванні та використанні інформаційних технологій, інфраструктури та інформаційних ресурсів, захисті інформації високого значення й прав суб’єктів, що беруть участь в інформаційній діяльності [7]. На думку Р. Калюжного, інформаційна безпека – це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов’язані з створенням, зберіганням, поширенням і використанням інформації [8]. К. Бєляков також зазначає, що під інформаційною безпекою слід розуміти не лише технологічну, але й правову захищеність інформаційної сфери суспільства, що забезпечує її формування та розвиток в інтересах громадян, організацій та держави в цілому [9].

Про інформаційну безпеку, як захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави, говорить Б. Кормич [10].

Ряд вчених [11] розглядають інформаційну безпеку як процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України. Через властивість управління загрозами і небезпеками пропонує розглядати інформаційну безпеку В. Шульга [12]. А. Лукашов в своїй праці [13] запропонував визначати інформаційну безпеку як функціонування системи засобів, що забезпечують захищеність інформаційних систем, котрі являють собою впорядковану сукупність інформаційних ресурсів, інформаційних технологій та комплексу програмно-технічних засобів, якими здійснюються інформаційні процеси в людино-машинному або автоматичному режимі. До цього, В. Брижко вважає, що під інформаційною системою розуміється така система, яка отримує вхідні дані або інформацію, здійснює їх обробку або зміну свого внутрішнього стану (зв’язків) та видає результати обробки для подальших дій [14 , с. 5].

Ю. Фісун характеризує інформаційну безпеку як стан захищеності інформаційного середовища, який відповідає інтересам держави, який забезпечує формування, використання і можливості розвитку незалежно від впливу внутрішніх і зовнішніх інформаційний загроз [15].

За визначенням І. Панаріна, інформаційна безпека – це стан інформаційного середовища суспільства і політичної еліти, що забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства [16, с. 128].

І. Бондар пропонує розглядати національну безпеку України в інформаційній сфері, тобто, інформаційну безпеку, як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки [17].

І. Громико визначає інформаційну безпеку як захищеність державних інтересів, за

якої забезпечується запобігання, виявлення і нейтралізація внутрішніх та зовнішніх інформаційних загроз, збереження інформаційного суверенітету держави і безпечний розвиток міжнародного інформаційного співробітництва [18, с. 134]

На думку О. Баранова, під інформаційною безпекою слід розуміти такий стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [19].

В. Остроухов також визначає інформаційну безпеку як стан захищеності об’єкта (особистості, суспільства, держави, інформаційно-технічної інфраструктури), при якому досягається його нормальне функціонування незалежно від внутрішніх і зовнішніх інформаційних впливів [20, с. 136].

Такі визначення, які можна назвати традиційними, в цілому відображають погляди багатьох інших дослідників та співвідносяться із законодавчим визначенням інформаційної безпеки, що наведене у Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки”. Так, зазначений Закон тлумачить інформаційну безпеку, як “стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації” [21].

Наведене визначення, як бачимо, не визначає співвідношення національної та інформаційної безпеки, а також не надає уявлення про систему інформаційної безпеки, так само, як і визначення, які торкаються окремих аспектів інформаційної безпеки, зокрема, інформаційної безпеки телекомунікаційних мереж [22] або кібербезпеки [23].

На доктринальному рівні система інформаційної безпеки вибудовується з використанням доволі широкого спектру критеріїв, що зумовлює диференціацію підходів до змісту поняття “система інформаційної безпеки”.

У зарубіжних наукових джерелах під системою інформаційної безпеки зазвичай розуміють систему безпеки інформації у складі таких структурних елементів, як цілісність, доступність та конфіденційність інформації [24 – 26]. Під цілісністю інформації розуміють її властивість не бути модифікованою неавторизованим користувачем і (або) процесом, тобто, зберігатись у стані, визначеному її створювачем та законним володільцем, в т.ч. й достовірність інформації як її відповідність дійсності в аспекті адекватності відображення. Конфіденційність означає властивість інформації бути недоступною користувачам, які не мають на це права. Ця властивість пов’язана з розмежуванням інформації за режимом доступу. Доступність інформації полягає в тому, що уповноважений користувач може використовувати її відповідно до правил, встановлених політикою безпеки, не очікуючи більше заданого проміжку часу, тобто це властивість інформації знаходиться у необхідному користувачеві вигляді та місці, в той час, коли вона йому необхідна [27, с. 190]. Втім відповідні характеристики не можуть надати уявлення про систему інформаційної безпеки як складової національної безпеки.

Натомість науковці пострадянського простору, в тому числі й вітчизняні вчені, приділяють значну увагу питанням інформаційно-психологічної та державно-ідеологічної складової інформаційної безпеки, існування яких зумовлюється поділом інформаційної сфери на інформаційно-технічну та інформаційно-психологічну [28, с. 62; 29-31]. На підставі критерію функціональності також пропонують визнавати складовими системи

інформаційної безпеки її аспекти: соціальний; нормативно-правовий; економічний; фінансовий; військовий; екологічний; програмно-технічний тощо [32, с. 74].

За твердженням Б. Кормича, інформаційна безпека має суб’єктно-об’єктний склад, відтак з точки зору критерію основного об’єкту система інформаційної безпеки складається з інформаційної безпеки особи, інформаційної безпеки суспільства та інформаційної безпеки держави. Крім того, держава, людина та суспільство одночасно виступають і як суб’єкти інформаційної безпеки, здійснюючи своїми діями захист важливої для них інформації та інформаційних процесів [33, с. 28-32].

О. Довгань розглядає інформаційні структури як компоненти інформаційної безпеки, тобто, як елементи системи інформаційної безпеки [34, с. 110-119], та вважає її об’єктом інформаційний суверенітет [35, с. 109-111]. Також систему інформаційної безпеки характеризують такі поняття, як інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології [36, с. 84].

О. Тихомиров зазначає, що інформаційна безпека – це стан інформаційної системи загалом та її елементів зокрема, що характеризується сукупністю умов оптимального функціонування і розвитку в інформаційній сфері та можливостями їх усвідомлення та контролю [37, с. 74], однак вибудовує систему забезпечення інформаційної безпеки за широким спектром критеріїв, зокрема: за сферами суспільного життя *(забезпечення інформаційної безпеки в економічній, політичній, воєнній, науково-технологічній, екологічній, соціальній сфері тощо)*; за об’єктами національної безпеки *(забезпечення інформаційної безпеки особи, суспільства та держави)*; за сучасними аспектами розуміння інформаційної безпеки *(забезпечення інформаційно-психологічної безпеки, забезпечення інформаційної безпеки у сфері прав і свобод людини та інформаційно-технічної, в т.ч. кібернетичної безпеки)*; за основними видами інформаційної діяльності *(забезпечення законних можливостей створення, збирання, одержання та використання інформації, законного порядку поширення інформації, належного зберігання інформації, охорона та захист інформації, створення і розвиток інформаційних ресурсів тощо)*; за формами державного забезпечення інформаційної безпеки *(забезпечення якісного інформування, процесів інформатизації; правова регламентація сфери інформаційних відносин; боротьба з правопорушеннями в інформаційній сфері*); за напрямами пізнавального процесу в галузі забезпечення інформаційної безпеки *(професійна освіта, наукові дослідження, інформаційно-просвітницька діяльність тощо)*; …за засобами забезпечення інформаційної безпеки: правове забезпечення *(правова регламентація відносин в інформаційній сфері; контрольно-наглядова діяльність, ліцензування, сертифікації, експертизи тощо)*; техніко-технологічне забезпечення; залежно від особливостей забезпечення доступу до інформації *(за правовим режимом доступу до інформації; за заходами із захисту секретної інформації тощо)* [38, с. 67-74].

На відмінності між системою інформаційної безпеки та системою забезпечення інформаційної безпеки можуть бути екстрапольовані відповідні закономірності, виявлені щодо системи національної безпеки та системи забезпечення національної безпеки [39, с. 5-8]. Так, основними елементами системи забезпечення інформаційної безпеки є її суб’єкти і об’єкти, а також прямі та зворотні зв’язки між ними. Основними об‘єктами системи забезпечення інформаційної безпеки як складової національної безпеки є національні цінності, національні цілі та національні інтереси. Розглядаючи національні цінності, національні інтереси та національні цілі через призму їх носіїв, можна класифікувати об‘єкти системи забезпечення інформаційної безпеки наступним чином: держава *(конституційний лад, суверенітет і територіальна цілісність України,*

політична, економічна та соціальна стабільність, законність і правопорядок, розвиток рівноправного взаємовигідного міжнародного співробітництва тощо); суспільство *(розвиток демократії, збереження культури і духовно-історичної спадщини, збереження і розвиток інформаційних ресурсів, досягнення й розвиток суспільної злагоди, політична стабільність, віротерпимість тощо)*; людина і громадянин *(життя, здоров‘я, культура, традиції тощо)*. Суб’єктами системи забезпечення інформаційної безпеки виступають держава (у т.ч. її інститути, посадові особи), суспільство (соціальні верстви та групи, громадські організації), а також окремі громадяни.

В. Ярочкин фактично ототожнює систему забезпечення інформаційної безпеки та систему інформаційної безпеки, адже пропонує під системою інформаційної безпеки розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства й держави від внутрішніх і зовнішніх загроз. Компонентами концептуальної моделі інформаційної безпеки (на прикладі безпеки інформації) за такого підходу визначаються: об’єкти загроз; загрози; джерела загроз; цілі загроз; джерела інформації; способи неправомірного заволодіння конфіденційною інформацією (способи доступу); напрямки захисту інформації; способи захисту інформації; засобу захисту інформації [40, с. 40-52].

О. Довгань пропонує модель системи забезпечення інформаційної безпеки, яка утворюється об’єктами інформаційної безпеки та суб’єктами інформаційної безпеки відповідно. При цьому *до об’єктів інформаційної безпеки* належать: конституційні права і свободи людини і громадянина, фізичне та психологічне здоров’я населення, захищеність людини від деструктивного та маніпулятивного інформаційного впливів; інформаційне забезпечення, гарантії інформаційних прав та права на розвиток населення всіх регіонів України; інформаційний суверенітет, безпека національного сегмента глобального інформаційного простору, інформаційної інфраструктури, захищеність, цілісність, доступність та безпечність інформаційних ресурсів, продукції і послуг. *До суб’єктів* забезпечення інформаційної безпеки у такій системі віднесені: Президент України, Верховна Рада України, Кабінет Міністрів України; Рада національної безпеки і оборони України, Національний банк України; Міністерство інформаційної політики України, Державний комітет телебачення і радіомовлення України, Національна рада України з питань телебачення і радіомовлення; Державна служба спеціального зв’язку і технічного захисту інформації України, Національна комісія України, що здійснює державне регулювання з питань зв’язку та інформатизації; Служба безпеки України, розвідувальні органи України, Державна прикордонна служба України, Збройні Сили України та інші військові формування, утворені відповідно до законів України; центральні органи виконавчої влади, місцеві органи державної влади та органи місцевого самоврядування, судові органи, прокуратура України та інші органи охорони правопорядку, віднесені законодавством до суб’єктів забезпечення національної безпеки України; засоби масової інформації, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність, наукові установи та вищі навчальні заклади України інформаційного профілю, інститути громадянського суспільства, громадяни України та інші особи (за згодою) [41, с. 13].

На думку В. Пилипчука, до основних суб’єктів системи забезпечення інформаційної безпеки, які мають забезпечувати або брати участь у розробці та реалізації державної інформаційної політики, слід віднести наступні: Міністерство інформаційної політики України; Міністерство юстиції України; Державний комітет телебачення і радіомовлення України; Національну раду України з питань телебачення і

радіомовлення; Державну службу спеціального зв’язку і захисту інформації України; Національну комісію, що здійснює державне регулювання у сфері зв’язку та інформатизації; інші державні й недержавні органи, заклади, установи, підприємства та організації. Найбільш актуальними проблемами інформаційної безпеки дослідник вважає, зокрема: проблему ефективності державної інформаційної політики та політики національної безпеки в інформаційній сфері; проблема забезпечення кібербезпеки; проблему захисту прав, свобод і безпеки людини і громадянина в інформаційній сфері [42, с. 25-26], що дозволяє скласти певне уявлення про систему інформаційної безпеки.

Досліджуючи питання забезпечення інформаційної безпеки, О. Баранов наголошує на необхідності забезпечення інформаційної безпеки у трьох її складових: забезпечення запобігання завдання шкоди через неповноту, невчасність та невірогідність інформації; забезпечення запобігання нанесення шкоди через негативний інформаційний вплив; забезпечення запобігання завданню шкоди через негативні наслідки функціонування інформаційних технологій [43, с. 33]. Система інформаційної безпеки, таким чином, утворюється безпекою інформації, безпекою від негативних інформаційних впливів, безпекою інформаційних технологій. Втім гуманітарна складова інформаційної безпеки містить у собі величезну сукупність проблем, пов’язаних з дотриманням конституційних прав і свобод громадян у сфері духовного розвитку й інформаційної діяльності. То ж безпека інформаційної сфери не може сприйматися суто як захист телекомунікаційних мереж або мереж зв’язку, засобів масової інформації від проникнення небажаної або шкідливої інформації. Про необхідність дослідження загроз інформаційній безпеці людини з точки зору її інформаційних прав та свобод вказує О. Золотар, наголошуючи на тому, що інформаційна безпека людини передбачає в т.ч. реалізацію життєво важливих інтересів людини та гармонійний розвиток в умовах інформаційного суспільства незалежно від наявності інформаційних загроз [44, с. 77].

Таким чином, оскільки метою забезпечення інформаційної безпеки є передусім попередження шкідливих інформаційних впливів та неправомірних дій щодо інформаційних ресурсів та інформаційних систем (біологічних, соціальних та технічних), захист прав та забезпечення реалізації інтересів суб‘єктів інформаційної сфери, а також забезпечення захищеності істотних властивостей інформації, нами вже обґрунтовувалася думка, що система інформаційної безпеки складається з безпеки інформації, безпеки від інформаційних впливів, а також захисту інформаційних прав та належного порядку реалізації інтересів суб’єктів інформаційної сфери [45, с. 155].

При цьому безпека інформації як захищеність її основних властивостей має забезпечуватись не лише щодо інформації з обмеженим доступом, але й іншої інформації, оскільки має бути відвернена не лише загроза порушення конфіденційності інформації, але й загроза порушення її цілісності та достовірності, а також і доступності інформації. Під безпекою від інформаційних впливів слід розуміти безпеку інформаційних систем та зв’язків між ними від інформаційних впливів, що здатні спричинити шкоду, в т.ч. й інформаційно-психологічну безпеку людини й суспільства. Забезпечення інформаційно-психологічної безпеки полягає в мінімізації негативних впливів на свідомість людини та суспільства, пов’язаних передусім із маніпулюванням свідомістю з різною метою, і поширенням суспільно небезпечної інформації, в тому числі деструктивної ідеології (культу насильства та жорстокості, расизму, радикального націоналізму, порнографії тощо) [37, с. 70-71]. Як вважає Брижко В.М., по суті, маніпуляція свідомості – це цензура, яка є засобом інформаційної боротьби, що обмежує свободу слова та порушує складні інформаційні системи, якими є людина, суспільство або держава [14, с. 7, 43-71].

Захист інформаційних прав та забезпечення реалізації інтересів суб’єктів інформаційної сфери як підсистеми інформаційної безпеки пов’язаний з двома іншими її складовими, оскільки мова йде передусім про потребу у безпечному інформаційному середовищі та права на інформацію. Якщо мова йде про інформаційну безпеку як про інформаційний вимір національної безпеки (мається на увазі стан не окремих структур, сторін або відносин нації), а її здатність ефективно функціонувати, незважаючи й всупереч негативним факторам не поступатися своїми інтересами під тиском зовнішніх, внутрішніх або комплексних загроз. Таким чином, категорія “інформаційна безпека” на національному рівні повинна відноситись до країни, до держави, що розуміється як органічна єдність території, населення й влади, і тлумачитися на холістичних засадах, виходячи з якісної своєрідності цілого стосовно до його частин. Ця своєрідність полягає в тому, що інформаційна безпека країни припускає й означає інформаційну безпеку всіх її структур і утворень, але допускає можливе ослаблення її для деяких з них. У той же час, зміцнення інформаційної безпеки окремих об’єктів, сегментів або сфер, узятих окремо, важливо для інформаційної безпеки як складової національної безпеки (її інформаційного виміру), але не створює її.

Отже, інформаційна безпека виступає як стан і умови життєдіяльності соціуму, які забезпечують сприятливі умови для розвитку особистості, суспільства й держави, а так само й інших об’єктів, тоді як інформаційна безпека кожного з цих об’єктів окремо виступає не як її частина, а як її мета та результат. У широкому сенсі інформаційна безпека повинна включати такі проблеми, як протистояння культурній експансії з боку країн з розвиненою аудіовізуальною промисловістю, збереження національної і мовної самобутності, нейтралізацію впливу недоброякісної, недостовірної, хибної інформації (дезінформації) на реалізацію національних інтересів. Слід звернути увагу й на те, що “безпека взагалі” не існує, адже атрибутом існування об’єкта будь-якої природи є наявність загроз, відтак модель системи інформаційної безпеки припускає визначення того, кому, що, чим загрожує, а також можливі механізми й способи протидії загрозливим факторам.

В. Пилипчук та О. Дзьобань відносять до основних видів загроз інформаційній безпеці наступні: витіснення вітчизняних інформаційних агентств, засобів масової інформації із внутрішнього інформаційного ринку та посилення залежності духовної, економічної і політичної сфер громадського життя України від закордонних інформаційних структур; маніпулювання інформацією (дезінформація, приховування чи перекручування інформації); інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на розробку і реалізацію зовнішньої політики держави; поширення за кордоном дезінформації про зовнішню політику України; порушення прав громадян і юридичних осіб в інформаційній сфері в Україні й за кордоном; спроби несанкціонованого доступу до інформації і впливу на інформаційні ресурси, інформаційну інфраструктуру органів державної влади, що реалізують державну зовнішню політику, українських представництв і організацій за кордоном, представництв України при міжнародних організаціях [46, с. 47-48].

Тому О. Дзьобань та О. Соснін обґрунтовано наголошують на необхідності постійного контролю стану безпеки в інформаційній сфері, ранжування загроз за ступенем впливу на національні інтереси, раціонального перерозподілу сил і засобів для нейтралізації загроз [47, с. 33].

Необхідно також враховувати, що зміст інформаційної безпеки не можна зводити тільки до захищеності – її зміст значно ширший. Забезпечення безпеки передбачає не тільки збереження певного існуючого стану, але й створення можливостей для виходу

на новий, якісно більш високий рівень розвитку. Відповідно, безпека – не стільки незмінний стан об’єкта, скільки його здатність відтворюватися, розбудовуватися, стало й прогресивно розвиватися в умовах конфліктів, невизначеності й ризику. Так само неприйнятним є визначення інформаційної безпеки як “захищеності інтересів”, адже інтереси – це потреби, без задоволення яких нормальне існування соціуму неможливо, то ж їх потрібно не захищати, а реалізовувати. Захисту потребують цінності, необхідні для нормальної життєдіяльності людини, суспільства, держави, і умови, що забезпечують їхній доступ до цих цінностей і можливість користуватися ними. Безпека припускає, насамперед, наявність необхідних цінностей і доступу до них. Відсутність цінностей вимагає пошуку їх нових джерел або їх замінників, а ускладнений доступ до них – усунення перешкод або вжиття заходів для їхнього подолання, що, у свою чергу, визначає зміст категорії “національні цілі”.

Таким чином, інформаційну безпеку України слід визначити як стан, за якого в умовах дії різнопланових загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, в т.ч. захищеність національних цінностей, необхідних для існування суверенної Української держави та виконання нею своїх функцій, а також досягнення відповідних національних цілей та реалізація національних інтересів. Інформаційна сфера при цьому утворюється сукупністю: суб‘єктів інформаційних процесів, інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, а також суспільних відносин, що складаються у зв‘язку з формуванням, зберіганням, передачею та розповсюдженням інформації. За такого визначення система інформаційної безпеки з точки зору її об’єктів відповідає класичній формулі для об’єктів національної безпеки “територія – народонаселення – система державного управління”, однак замість території для інформаційної безпеки вважаємо за доцільне використовувати поняття “інформаційний простір”, яке в т.ч. охоплюватиме інформаційну модель території та її інформаційне обслуговування.

Відповідно, функціональна система інформаційної безпеки України як складової та інформаційного виміру національної безпеки матиме наступний вигляд, див. далі на Рис.

На нашу думку, розмежування інформаційної безпеки як стану динамічної системи та забезпечення інформаційної безпеки як процесу підтримання цього стану (включаючи самовідтворення, збереження та розвиток) дозволяє певним чином зняти протиріччя між організаційно-структурним і функціонально-діяльнісним підходами до визначення сутності феномену інформаційної безпеки та її системи. То ж система інформаційної безпеки як певне утворення, що характеризується подільністю, відкритістю, адаптивністю та наявністю структури, мети й пріоритетів оптимальної взаємодії елементів [48, с. 86], виступає об’єктом для системи забезпечення інформаційної безпеки, до якої також входять сили й засоби забезпечення інформаційної безпеки.

Зауважимо, що система інформаційної безпеки, особливо на рівні її результуючих компонентів, може бути структурована за різними критеріями. На жаль, на законодавчому рівні питання системи інформаційної безпеки досі системно не вирішено. Навіть нова Доктрина інформаційної безпеки України [49], яка готувалася в умовах, коли наша країна потерпає від гібридної агресії Російської Федерації, а отже – вже потрібно було б усвідомлювати значення інформації, інформаційних впливів та інформаційної сфери в цілому, не орієнтує на вирішення усього комплексу виявлених проблем, не загострює проблеми необхідності їх законодавчого врегулювання.

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу РФ в умовах розв’язаної нею гібридної війни. Доктрина визначає національні інтереси

України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Її правовою основою є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента від 26 травня 2015 року № 287 [22], а також міжнародні договори, згода на обов’язковість яких надана Верховною Радою України.

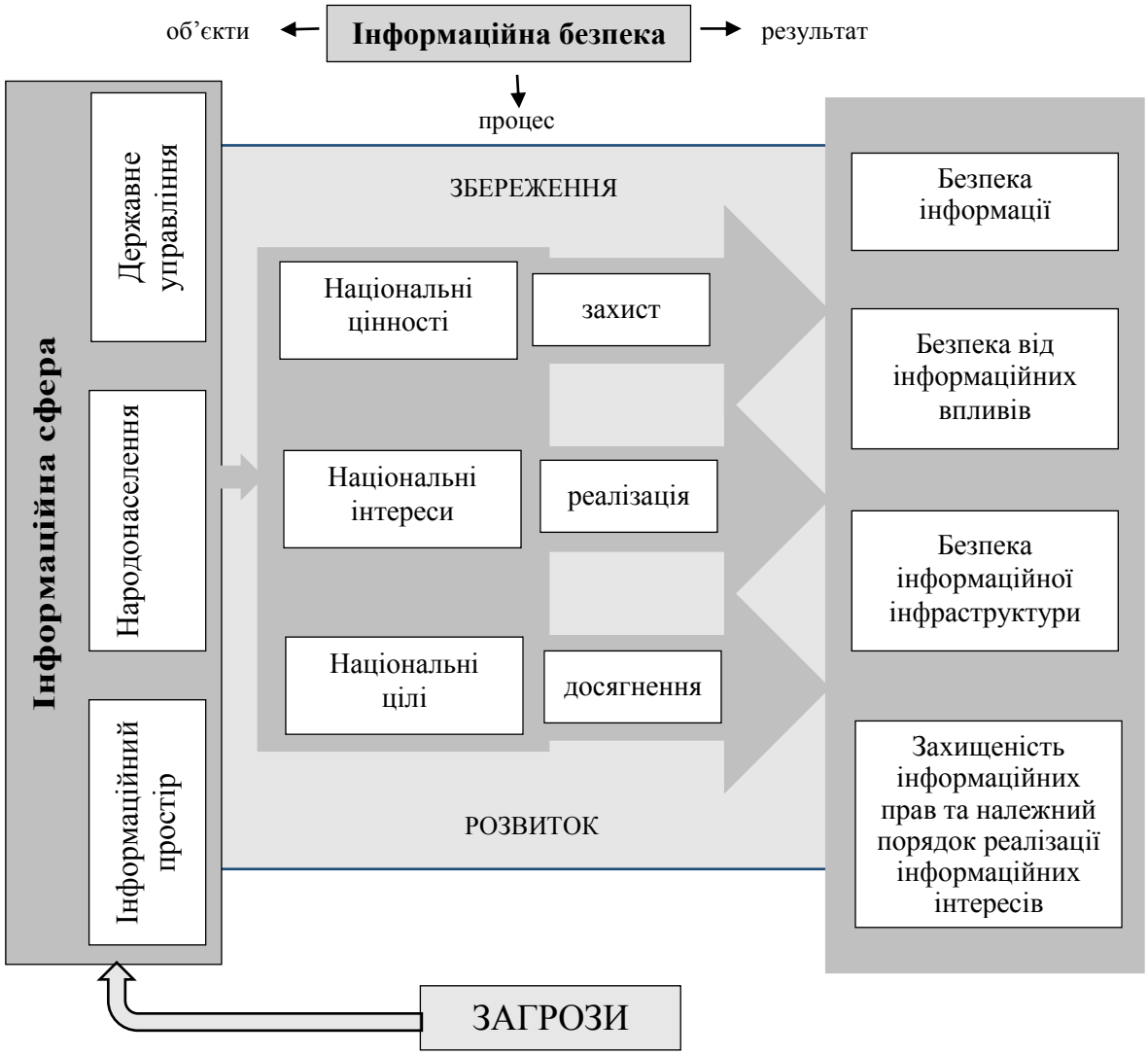

Рис. Система інформаційної безпеки

У тексті Доктрини йдеться про національні інтереси України в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці, пріоритети державної політики в інформаційній сфері і механізм реалізації доктрини. Доктриною передбачається захист українського суспільства від “агресивного інформаційного впливу Російської Федерації”, розвиток публічної дипломатії, в тому числі культурної та цифрової, видалення шкідливої інформації з українського сегменту інтернету та квотування національного аудіовізуального контенту, захист права на вільний доступ до інформації, створення механізмів захисту від пропаганди тощо.

Втім, у експертному середовищі Доктрина отримала переважно негативну оцінку на кшталт “Доктрина інформаційної безпеки України – це лише декларація” або “замість інтеграції Україна встановлює паркан” тощо [50]. Дійсно, у Доктрині держава виклала бачення розвитку й функціонування свого інформаційного простору і визначила, що

Російська Федерація є супротивником, який веде системну інформаційну війну. У документі є пропозиції, як реагувати на агресію та забезпечувати інформацією громадян. Доктрина також визначає поняття “стратегічного наративу” і вказує, що медіа мають самі себе регулювати, але при цьому повинні нести соціальну відповідальність. Втім, Доктрина закладає державну систему постійного моніторингу веб-ресурсів та блокування сайтів, що загрожують безпеці, однак підстави для блокування доволі абстрактні – орган державної влади на свій розсуд зможе тлумачити, що загрожує безпеці, а що – ні. Відповідно, виникає небезпека встановлення цензурованих шлюзів, які відокремлять український інтернет від світу. Крім того, механізм реалізації Доктрини навіть у її позитивних аспектах не містить жодної конкретики, тож у чинній редакції Доктрина не може слугувати базовим документом, на підставі якого мають формуватися і інші правові акти у сфері забезпечення інформаційної безпеки, в тому числі стратегічні та програмні документи.

Ми цілком поділяємо думку О. Довганя, який слушно зазначає, що сьогодні в черговий раз потрібно піднімати питання щодо розробки нормативного акту (закону), яким буде визначено єдиний понятєво-категорійний апарат, державну політику забезпечення інформаційної безпеки, об’єкти інформаційної безпеки та суб’єкти її забезпечення, правові зони відповідальності відомств, залучених до сфери забезпечення інформаційної безпеки, механізми координування їх діяльності щодо реагування на виклики та загрози національній безпеці в інформаційній сфері, порядок правового закріплення взаємовідносин державних безпекових структур із іншими органами та відомствами, віднесеними законодавством до суб’єктів забезпечення національної безпеки України тощо [51, с. 37-38]. Вважаємо, що такий нормативний акт обов’язково має визначати як систему інформаційної безпеки, так і систему забезпечення інформаційної безпеки.

З цього приводу зазначимо, що на засіданні РНБО України 17 січня 2018 року члени РНБО обговорили та підтримали проект Закону України “Про національну безпеку України”, який, за повідомленням офіційного сайту РНБО, “розроблявся у тісній взаємодії з експертами НАТО, США та Європейського Союзу з метою приведення української законодавчої бази у відповідність до стандартів держав-членів НАТО” [52]. На жаль, за результатами аналізу цього проекту слід дійти висновку, що він не відповідає вимогам нормопроектувальної техніки, передусім: базується на підміні понять “суспільна безпека” (“соціальна безпека”) у розумінні “безпека суспільства” та “громадська безпека”; передбачає “точкове” регулювання відносин щодо окремих об’єктів, що входять до систем, перелік складових яких є невичерпним (зокрема, систем на кшталт суспільної безпеки, національної безпеки, системи державних органів, які беруть участь у забезпеченні національної безпеки тощо); містить положення, які не стосуються предмета регулювання, задекларованого в назві проекту та суперечливі норми права, дублює і повторює норми права, які містяться в інших нормативно-правових актах. Проект також не містить визначення основоположних дефініцій у сфері забезпечення національної безпеки, зокрема таких, як “національні цінності”, “національні цілі”, “система забезпечення національної безпеки”, “система національної безпеки”, “вид (сфера) національної безпеки”, “об’єкти національної безпеки”, “основи національної безпеки” тощо, а відтак не може слугувати підґрунтям для визначення відповідних понять у контексті забезпечення інформаційної безпеки.

Натомість, актуалізується нагальна потреба у розробці та прийнятті Закону України “Про інформаційну безпеку України” як базового закону, що регулюватиме

питання інформаційної безпеки. Таким закон, як підґрунтя ефективної стратегії інформаційної безпеки, повинен містити не абстрактні декларації, а чітко визначені основоположні категорії у сфері інформаційної безпеки та підходи до формування системи забезпечення інформаційної безпеки, механізм її функціонування, повноваження і схему взаємодії суб’єктів забезпечення інформаційної безпеки тощо.

Висновки.

Створення належних умов для реалізації державної політики, спрямованої на захист національних цінностей та реалізацію національних інтересів України, гарантування безпеки особи, суспільства і держави від зовнішніх та внутрішніх загроз в інформаційній сфері, потребує формування сучасних ефективних механізмів забезпечення інформаційної безпеки, які відповідатимуть характеру і масштабам викликів сьогодення. Складна воєнно-політична, оперативно-стратегічна та економічна ситуація, яка склалася внаслідок збройної агресії Російської Федерації проти нашої держави, набула загрозливих проявів у інформаційному просторі.

Відповідно, надзвичайно актуальним стає доктринальне та нормативне визначення такої основоположної категорії, як “система інформаційної безпеки”, адже інформаційна безпека є системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники, зокрема, політична обстановка у світі; внутрішньополітична обстановка в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо. Важливим для цього вважаємо розмежування інформаційної безпеки як стану динамічної системи та забезпечення інформаційної безпеки як процесу підтримання цього стану (включаючи самовідтворення, збереження та розвиток) дозволяє зняти протиріччя між організаційно-структурним і функціонально-діяльнісним підходами до визначення сутності феномену інформаційної безпеки та її системи.

У методологічному відношенні важливо не тільки перелічити складові системи інформаційної безпеки, але й доповнити вербалізацію цих явищ операціоналізацією і концептуалізацією понять, що їх позначають. Отже, наразі набуло непересічної актуальності питання розробки та прийняття Закону України “Про інформаційну безпеку України” як базового закону, що регулюватиме питання інформаційної безпеки.

Використана література

1. Конституція України : Закон України від 28.06.96 р. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/254к/96-вр. – Дата звернення 18.02.2018 р.

2. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. – Режим доступу : http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php. – Дата звернення 18.02.2018 р.

3. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / В. Ліпкан, Ю. Максименко, В. Желіховський. – К. : КНТ, 2006. – 280 с.

4. Данильян О.Г. Національна безпека України : структура та напрямки реалізації : навчальний посібник / О. Данильян, О. Дзьобань, М. Панов. – Х. : Фоліо, 2002 – 285 с.

5. Гурковський В.І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства // Правова інформатика. – 2010. – № 2(26). – С. 72-77.

6. Нижник Н. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навчальний посібник / Н. Нижник, Г. Ситник, В. Білоус. – Ірпінь : Акад. ДПС України, 2000. – 304 с.

7. Ярочкин В.И. Словарь терминов и определений по безопасности и защите информации / В. Ярочкин, Т. Швецова. – М. : Ось-89, 1996. – 48 с.

8. Питання концепції реформування інформаційного законодавства України / Р. Калюжний та ін. // Правове, нормативне та метрологічне забезпечення системи інформації в Україні : тематичний зб. праць учасників 2-ї науково-технічної конференції. – К., 2000. – С. 17-21.

9. Бєляков К.І. Деякі питання щодо формування реформи інформаційного законодавства України : мат. міжнародної науково-практичної конференції [“Систематизація законодавства в Україні : проблеми теорії і практики”]. – К. : Інститут законодавства Верховної Ради України, 1999. – С. 253-255.

10. Кормич Б.А. Інформаційна безпека : організаційно-правові основи : навчальний посібник / Б.Кормич. – К. : Кондор, 2004. – 382 с.

11. Ліпкан В.А., Харченко Л.С., Логінов О.В. Інформаційна безпека України : глосарій. – К. : Текст, 2004. – 136 с.

12. Шульга В.І. Сучасні підходи до трактування поняття інформаційна безпека / Ефективна економіка. – 2015. – № 4. – Режим доступу : http:// http://www.economy.nayka.com.ua/ ?op=1&z=5514. – Дата звернення 19.02.2018 р.

13. Лукашов А.И. Информационная безопасность как объект уголовно-правовой охраны в законодательстве Республики Беларусь : мат. научной конференции [“Концептуальные проблемы информационной безопасности в союзе России и Беларуси”]. – СПб., 2000. – Режим доступу : http://jurfak.spb.ru/conference/2001.htm. – Дата звернення 19.02.2018 р.

14. Брижко В.М. е-боротьба в інформаційних війнах та інформаційне право : монографія / В.М. Брижко, М.Я. Швець. – К. : НДЦПІ АПрН України, 2007. – 239 с.

15. Фисун Ю.А. Вопросы информационной безопасности личности, общества и государства накануне 21 века : мат. международной конференции [“Информатизация правоохранительных систем”], (м. Москва, 7 – 8 июня 2000 г.). – М., 2000, – С. 86-92.

16. Панарин И. Технология информационной войны : монографія / И. Панарин. – М. : “КСП+”, 2003. – 320 с.

17. Бондар І.Р. Інформаційна безпека як основа національної безпеки / Mechanism of Economic Regulation. – 2014. – № 1. – С. 68-75.

18. Громико І., Саханчук Т. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам // Право України. − 2008. − № 8. – С. 130-134.

19. Баранов А.А. Концептуальные вопросы информационной безопасности Украины : сб. материалов [“Нормативно-правовая база защиты информации”]. – К., 1997. – С. 53-58.

20. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України // Політичний менеджмент. – 2008. – № 4. – С. 135-141.

21.Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. – Режим доступу : zakon5.rada.gov.ua/laws/show/537-16. – Дата звернення 13.02.2018 р.

22. Про телекомунікації : Закон України від 18.11.03 р. – Режим доступу : zakon2.rada.gov.ua/laws/show/1280-15. – Дата звернення 13.02.2018 р.

23. Про рішення Ради національної безпеки і оборони України від 27.01.16 р “Про Стратегію кібербезпеки України” : Указ Президента України від 15.03.16 р. № 96/2016. – Режим доступу: www.president.gov.ua/documents/962016-19836. – Дата звернення 20.08.2018 р.

24. Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security. – Online tool. – Available at : https://doi.org/10.6028/NIST.SP.800-12r1. – Accessed 04.10.2017.

25. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec) – Online tool. – Available at : //www.cnss.gov/Assets/pdf/nstissi_4011.pdf. – Accessed 04.10.2017.

26. Federal Financial Institutions Examination Council (FFIEC). Information Technology Examination Handbook (IT Handbook) : Information Security (2016). – Online tool. – Available at : https://www/ffiec.gov/press/pdf/ffiec-it-handbook_information_security_booklet.pdf. – Accessed 04.10.2017.

27. Мельник С.В. Понятійно-категоріальний аппарат у системі професійної підготовки майбутніх фахівців з кібербезпеки // Інформаційні технології і засоби навчання. – 2016 – Т. 55. – № 5 – С. 187-197.

28. Баришполец В.А. Информационно-психологическая безопасность : основные положения / РЭНСИТ : Информационные технологии. – 2013 – № 2. – Т 5. – С. 62-104.

29. Николаев А. Государственно-идеологическая компонента информационной безопасности. – Режим доступу : https://cyberleninka.ru/acticle/v/gosudarstvenno-ideologicheskaya-komponenta-informatsionnoy-bezopasnosti. – Дата звернення 15.02.2018 р.

30. Гулай В.В. Загрози інформаційно-психологічній безпеці особи в реаліях інформаційно-психологічної війни як складової “гібридної війни” Російської Федерації проти України. – Режим доступу : //www.asv.ua/content/nauka/editions/25/2016-25/233-244.pdf. – Дата звернення 16.02.2018 р.

31. Уханова Н.С. Інформаційно-психологічна безпека особистості, суспільства та держави. – Режим доступу : //www.ippi.org.ua/ukhanova-ns-informatsiino-psikhologichna-bezpekaosobistosti-suspil stva-ta-derzhavi. – Дата звернення 16.02.2018 р.

32. Жатканбаева А.Е. Функциональные компоненты информационной безопасности // Право и государство. – 2013. – № 4 (61) – С. 73-77.

33. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : монографія / Б.Кормич. – Одеса : Юридична література, 2003. – 472 с.

34. Довгань О.Д. Сучасні інформаційні структури як компоненти інформаційної безпеки // Інформація і право. – № 2(14)/2015. – С. 111-120.

35. Довгань О.Д. Національний інформаційний суверенітет – об’єкт інформаційної безпеки // Інформація і право. – № 3(12)/2014. – С. 102-112.

36. Довгань О.Д. Нейтралізація міжнародних інформаційних загроз // Правова інформатика. – № 2(42)/2014. – С. 80-89/

37. Тихомиров О.О. Перспективи зміни розуміння інформаційної безпеки // Правова інформатика. – № 4(28)/2010. – С. 68-75.

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

39. Концептуальні засади розвитку системи забезпечення національної безпеки України : аналіт. доп. / [О.О. Резнікова, В.Ю. Цюкало, В.О. Паливода, С.В. Дрьомов, С.В. Сьомін]. – К. : НІСД, 2015. – 58 с.

40. Ярочкин В.И. Информационная безопасность : учебное пособие для студентов непрофильных вузов.. – М. : Междунар. отношения, 2000. – 400 с.

41. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України // Інформаційна безпека людини, суспільства, держави. – 2015, № 3 (19). – С. 6-17.

42. Пилипчук В.Г. Забезпечення інформаційної безпеки України : сучасні тенденції та проблеми : матеріали наук.-практ. конф. [“Запобігання новим викликам та загрозам інформаційній безпеці України : правові аспекти”], (м. Київ, 6 жовт. 2016 р.) ; упоряд. : В.М. Фурашев. – К : Вид-во “Політехніка”, 2016. – С. 24-28.

43. Баранов О.А. Базовий принцип інформаційного права – забезпечення інформаційної безпеки : матеріали наук.-практ. конф. [“Запобігання новим викликам та загрозам інформаційній безпеці України : правові аспекти”], (м. Київ, 6 жовт. 2016 р.) ; упоряд. : В.М. Фурашев. – К : Вид-во “Політехніка”, 2016. – С. 29-35.

44. Золотар О.О. Загрози інформаційній безпеці людини // Правова інформатика. – № 2(42)/2014. – С. 70-79.

45. Ткачук Т. Складники інформаційної безпеки : аналіз критеріїв / Visegrad journal on human rights. – 2017 (4). – С. 153-158.

46. Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці в інформаційній сфері // Вісник Національної академії правових наук України. – № 3 (78) 2014. – С. 43-52.

47. Дзьобань О.П., Соснін О.В. Інформаційна безпека: нові виміри загроз, пов’язаних з інформаційно-комунікаційною сферою / Гуманітарний вісник ЗДІА. – 2015. – № 60 – С. 25-34.

48. Могилевский В.Д. Системная безопасность: формализованный подход : мат. конференции [“Проблемы внутренней безопасности России в XXI веке”]. – М. : ЭДАС-ПАК, 2001. – С. 86-89.

49. Про рішення Ради національної безпеки і оборони України від 29.12.16 р. “Про Доктрину інформаційної безпеки України” : Указ Президента України від 25.02.17 р. № 47/2017. – Режим доступу : //www.president.gov.ua/documents/472017-21374. – Дата звернення 20.02.2018 р.

50. Доктрина інформаційної безпеки України – це лише декларація – експерти. – Режим доступу : https://www.radiosvoboda.org/a/28336852.html. – Дата звернення 21.08.2018 р.

51. Довгань О.Д. Інформаційна безпека : стан, проблеми, тенденції : матеріали круглого столу [“Інформаційні ресурси, інтелектуальна власність, комунікації в освітньо-науковій та інноваційній сферах : філософсько-правові та прикладні аспекти”], (м. Вінниця, 12 травня 2017 р.) : упоряд. О.Д. Довгань, М.В. Беланюк, С.А. Лапшин, О.Г. Радзієвська, О.І. Яременко. – К. : Видавничий дім “АртЕк”, 2017. – С. 31-39

52. Про рішення Ради національної безпеки і оборони України від 17.01.18 р. “Про проект Закону України “Про національну безпеку України” : Указ Президента України від 5.02.18 р. № 21/2018. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/21/2018/ paran2#n2. – Дата звернення 22.08.2018 р.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~