

3. Незаконний видобуток піску на Волині – з подачі влади. Газета «Волинські новини» від 27 червня 2014 року // [Електронний ресурс]. – Режим доступу: <https://www.volynnews.com/news/authority/nezakonnyy-vydobutok-pisku-na-volyni-z-podachi-vlady/>.

4. Світличний О.П. Адміністративні правовідносини у сфері земельних ресурсів України: дис. ... на здобуття наук. ступ. док. юрид. наук. / О.П. Світличний. – К., 2012. – 440 с.

5. Афанасієв Р.В. Адміністративно-правові засоби забезпечення права власності на природні ресурси: поняття, сутність, істотні ознаки / Р.В. Афанасієв // Юридична Україна. – 2008. – № 8. – С. 17–22.

6. Крижанівська В.А. Адміністративна відповідальність в адміністративному праві України: сучасне розуміння, нові підходи: автореф. дис. ... канд. юрид. наук. / В.А. Крижанівська. – Львів. – 22 с.

7. Галуцько В.В. Методи переконання і примусу при здійсненні охорони власності / В.В. Галуцько // Держава і право. – 2006. – № 33. – С. 192–196.

УДК 342.9

МИРОШНИЧЕНКО М.М.

ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Статтю присвячено визначенню особливостей правового забезпечення інформаційної безпеки держави. Проаналізовано низку законодавчих актів, за допомогою яких здійснюється регулювання інформаційної безпеки держави. Ними встановлено низку суперечностей між ними та запропоновано шляхи покращення вітчизняного законодавства.

Ключові слова: інформаційна безпека, національна безпека, інформаційне середовище, інформаційний простір, правове забезпечення.

Статья посвящена определению особенностей правового обеспечения информационной безопасности государства. Проанализирован ряд законодательных актов, с помощью которых осуществляется регулирование информационной безопасности государства. Нами установлен ряд противоречий между ними и предложены пути улучшения отечественного законодательства.

Ключевые слова: информационная безопасность, национальная безопасность, информационная среда, информационное пространство, правовое обеспечение.

The article is devoted to the definition of the peculiarities of the legal security of the state information security. A number of legislative acts are analyzed, with the help of which the information security of the state is regulated. We have identified a number of contradictions between them and suggested ways to improve domestic legislation.

Key words: information security, national security, information environment, information space, legal support.

Вступ. Проблема правового забезпечення інформаційної безпеки держави набуває особливої актуальності саме сьогодні, адже реалізація та використання інформаційних технологій відбувається у всіх сферах життєдіяльності. Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. У ХХІ столітті обов'язковою умовою розвитку суспільства та держави є формування розвиненого і захищеного інформаційного середовища. Розвиток сучасних інформаційних технологій забезпечує впровадження передових змін у сфері управління

державотворчими процесами. Водночас посилюється небезпека несанкціонованого втручання в роботу найважливіших інформаційних систем, що може призвести навіть до катастрофічних наслідків. Прикладом може слугувати керування енергоблоками атомних електростанцій, що здійснюється за допомогою найновішого інформаційно-технічного обладнання. Саме тому більшість держав активно використовує найкращі людські та матеріальні ресурси для вирішення проблем захисту інформації та пошуку шляхів їх вирішення.

Постановка завдання. У чинному законодавстві нашої держави питанням інформаційної безпеки приділяється набагато менше уваги, ніж проблематиці побудови теоретичних моделей інформатизації в Україні та інформаційного суспільства. Частково ця ситуація пояснюється тим, що у національному законодавстві присутні два різні за своєю суттю визначення поняття «інформаційна безпека». Зокрема це поняття визначається у Законах України «Про телекомунікації» та «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». У Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» під указаною дефініцією розуміється інформаційна безпека нашої держави, яка визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігають нанесенню 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. У Законі України «Про телекомунікації» під час аналізу інформаційної безпеки держави увага приділяється переважно технічному боку питання, тобто інформаційна безпека телекомунікаційних мереж визначається їхньою здатністю забезпечувати захист від знищення, перекручування, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації [1].

На жаль, у базовому нормативно-правовому акті, який регулює інформаційну сферу держави, а саме Законі України «Про інформацію», визначення інформаційної безпеки держави відсутнє. Водночас у Законі України «Про основи національної безпеки України», інформаційна безпека розглядається обов'язковим складником національної безпеки України, але точне визначення цього поняття не наводиться і використовується формулювання «національна безпека України в інформаційній сфері».

У Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» також визначаються переважно технічні питання для забезпечення інформаційної безпеки держави у сфері інформатизації та телекомунікації, поняття інформаційної безпеки не знаходить свого відображення, але широко вживається поняття «захист інформації» [2]. Так, Закон України «Про Концепцію Національної програми інформатизації» визначає, що інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складників національної безпеки [3]. Таким чином, забезпечення захисту інформаційного простору та забезпечення інформаційної безпеки держави, а також захист прав і свобод фізичних осіб, визначається державою як пріоритетні завдання державної інформаційної політики [4].

Результати дослідження. Інформаційна безпека на нормативно-правовому рівні закріплюється як державна інформаційна політика. Також важливим є збереження державного впливу на стратегічні об'єкти інформаційної інфраструктури; забезпечення інформаційного суверенітету держави; організація вільного доступу до інформаційних ресурсів; розвиток інформаційної інфраструктури; постійна модернізація інформаційної сфери; посилення діяльності українських ресурсів у світовому інформаційному просторі; налагодження ефективної співпраці з іншими державами (зокрема державами-членами Європейського Союзу) в інформаційній сфері; забезпечення прав усіх суб'єктів інформаційних правовідносин; обмеження впливу іноземних держав чи потужних зарубіжних структур на вітчизняний інформаційний простір; посилення охорони державної таємниці та іншої важливої інформації [5, с. 144–145].

Державна діяльність в інформаційній сфері має визначатися важливістю національних інтересів, а також створенням відповідних правових засобів для досягнення цієї мети. У Законі України «Про основи національної безпеки України» визначено основні напрями державної політики щодо національної безпеки в інформаційній сфері. До них належать такі: забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації та журналістів, заборони цензури, дискримінації в інформаційній сфері й переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику; забезпечення інформаційного суверенітету України; активне

залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України; удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, упровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України. Слушною є позиція В.А. Ліпкана, який стверджує, що для організації та побудови продуманої державної політики в інформаційній сфері необхідне одночасне використання всіх об'єктів інформаційної інфраструктури. Інформаційний компонент національної безпеки України має забезпечуватися сукупністю державних органів, громадських організацій та окремих громадян [6, с. 116–117].

Варто зазначити, що питанням інформаційної безпеки приділяють значну увагу в підзаконних нормативно-правових актах. Одна з Програм діяльності Уряду наголошує, що ключовими завданнями є розвиток і вдосконалення системи гарантування інформаційного суверенітету та інформаційної безпеки держави, запобігання злочинам у сфері інформаційних технологій. Інша Програма визначає забезпечення реалізації конституційних прав громадян на свободу слова та інформації, розвиток державного інформаційного ресурсу, захист інформаційної безпеки та національних інтересів в інформаційній сфері. Проте в жодному з документів, затверджених Кабінетом Міністрів України (далі – КМУ), не наведено тлумачення чи роз'яснення терміна інформаційної безпеки держави. У рішенні Національної ради України з питань телебачення і радіомовлення інформаційна безпека згадується лише у назві відповідного рішення [7, с. 9–13].

Укази Президента України також широко застосовують поняття «інформаційна безпека». Проте переважно про інформаційну безпеку лише згадується у назвах чи преамбулах, тоді як у самому тексті термін «інформаційна безпека» практично не застосовується. Так, наприклад, в одному із Указів Президента України про інформаційну безпеку лише згадується у назві, а в тексті самого рішення Ради національної безпеки та оборони України (далі – РНБО), який цей Закон уводить у дію, замість терміна «інформаційна безпека» широко застосовується термін «національна безпека в інформаційній сфері» [8].

Також Указом Президента України затверджена Доктрина інформаційної безпеки України, яка виступає базовим системоутворюючим нормативним документом у сфері правового забезпечення інформаційної безпеки, який повинен повністю регламентувати діяльність держави, суспільства та громадян України щодо її забезпечення у цій сфері.

Варто зазначити, що у відомчих нормативно-правових актах та інших документах державних органів, які забезпечували або забезпечують в Україні захист інформації, зокрема в Департаменті спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України та Державної служби спеціального зв'язку та захисту інформації України, термін «інформаційна безпека» також не визначається, хоча широко використовується.

Значне місце було приділено інформаційній безпеці у проекті Концепції національної інформаційної політики України, що був розроблений Державним комітетом інформаційної політики, телебачення і радіомовлення [9]. На жаль, ця Концепція не була прийнята.

Як бачимо, більшість прикладних питань інформаційної безпеки визначається Доктриною інформаційної безпеки України. У ній визначаються національні інтереси України в інформаційній сфері, що поділяються на життєво важливі інтереси особи та життєво важливі інтереси суспільства й держави. До перших належать такі: забезпечення прав і свобод осіб в інформаційній сфері; збереження прав людини на захист особистого життя; захист від негативних інформаційних впливів. До других – мінімізація впливу іноземної пропаганди; недопущення діяльності інформаційних ресурсів, що загрожують територіальній цілісності та суверенітету нашій державі; повноцінне та своєчасне інформування осіб про ситуацію в державі; розвиток та захист вітчизняної інформаційної інфраструктури; посилення заходів для встановлення національної ідентичності; вирішення мовних питань; організація захисту мов національних меншин та сприяння вивченню мов міжнародного спілкування; встановлення більш тісних зв'язків з українською діаспорою; активізація інформаційного впливу на сучасне покоління; організація правової системи захисту особи, суспільства та держави від негативних зовнішніх впливів; налагодження співпраці з іншими державами для створення міжнародних механізмів захисту від негативних зовнішніх інформаційних впливів; всебічна інтеграція у європейський і світовий інформаційний простір; взаємодія з громадськістю під час формування, реалізації державної політики в ін-

формаційній сфері; забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України; захист державно-цінної інформації від несанкціонованого доступу; формування позитивного іміджу України у світі; впровадження вітчизняних іншомовних каналів у світовий інформаційний простір. Тобто цей правовий документ присвячується захисту інформаційної безпеки суспільства та держави. Інформаційній безпеці особистості приділяється увага лише поверхнево.

Позитивним є те, що у Доктрині визначаються пріоритети державної інформаційної політики, до яких належать питання інформаційної безпеки; захисту інформаційного простору; захисту прав осіб на інформацію; підтримання позитивного міжнародного іміджу нашої держави. У цьому документі деталізується низка понять та засобів для вирішення поставлених завдань щодо розбудови інформаційної безпеки держави, вводиться термін «інформаційний простір». Позитивним є те, що прописується відповідний механізм реалізації, який реалізовується визначеним колом суб'єктів. До них належать такі: КМУ, РНБО, Міністерство інформаційної політики України, Міністерство закордонних справ України, Міністерство оборони України, Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, СБУ, Розвідувальні органи України, Державна служба спеціального зв'язку та захисту інформації України, Національний інститут стратегічних досліджень. Крім того, визначаючи важливість забезпечення інформаційної безпеки держави та для сприяння координації діяльності органів виконавчої влади у сфері забезпечення інформаційного суверенітету України та взаємодії з іншими державними органами в інформаційній сфері у Міністерстві інформаційної політики України може утворюватися допоміжний орган. Також визначається, що суб'єкти реалізації державної інформаційної політики, у взаємодії з інститутами громадянського суспільства в межах компетенції, забезпечують реалізацію Доктрини, а також уносять обґрунтовані пропозиції щодо корегування її положень.

Щодо слабких сторін Доктрини, то можемо відмітити те, що у ній відсутнє визначення терміна «інформаційна безпека». Також не прописані основні цілі та завдання забезпечення інформаційної безпеки в Україні, не закріплюється необхідність вирішення на державному рівні актуальних проблем і завдань у сфері інформаційної безпеки. Не додає державній ваги документу і те, що у прикінцевих положеннях Доктрини лише прописано, що вона є основою для формування державної політики у сфері інформаційної безпеки України; розроблення проєктів концепцій, стратегій, цільових програм і планів дій із забезпечення інформаційної безпеки України; підготовки пропозицій щодо дальшого системного вдосконалення правового, методичного, науково-технічного і організаційного забезпечення інформаційної безпеки України.

До правової основи забезпечення інформаційної безпеки України також належить низка міжнародних документів, що були належним чином ратифіковані або парафоровані Україною. Серед них зазначимо такі: Договір про безпеку і співробітництво в Європі, Договір «Відкрите небо», Угода про партнерство і співробітництво між європейським співтовариством і Україною, Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства. Згадані документи носять декларативний характер та лише зобов'язують держави-учасниці здійснювати багатосторонній обмін інформацією, а також наголошують на реалізації нагальної потреби створення загальнодержавних механізмів зберігання та споживання отриманої інформації в національних інтересах.

Проте необхідно зауважити, що досі в Україні не прийнято закону, який би визначав концепцію державної інформаційної політики України. Тому в державі не існує єдиного плану, єдиної державної позиції чи стратегії розвитку інформаційної галузі, а отже, і забезпечення інформаційної безпеки. Лише після подій 2013–2014 років питанням інформаційної безпеки почала приділяється більша увага. Зокрема Указом Президента України було оприлюднене рішення РНБО «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». У цьому документі було передбачено здійснення багатьох дій найближчим часом, зокрема він стосувався діяльності КМУ, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Міністерства закордонних справ України. Але більшість прописаних намірів залишилися не виконаними навіть дотепер [10]. Пізніше було створено Міністерство інформаційної політики України. При Міністерстві в процесі спілкування Міністра з представниками громадськості була створена Експертна Рада, метою якої стало розроблення Стратегії інформаційної політики України, Концепції інформаційної безпеки України та Державної програми розвитку інформаційного простору України [11].

Досить часто прогресивні наукові дослідження не використовуються у законодавчих актах. У проєкті Закону «Про інформаційний суверенітет та інформаційну безпеку України» інформаційна безпека визначається як захищеність життєво важливих інтересів суспільства, держави і особи, якою виключається заподіяння шкоди через неповноту, несвочасність, недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок розповсюдження інформації, забороненої для розповсюдження законами України [12]. Зазначимо, що представлене у проєкті визначення є досить переобтяженим та виражає бажання держави контролювати всі інформаційні потоки, до яких вона може мати доступ. Недоцільним є структуризація інформації на «достовірну», «недостовірну», «зіпсовану». Уважаємо, що такий контроль є недоцільним та не сприяє демократизації суспільства, зокрема у сфері інформаційних правовідносин. Як бачимо, досить активний розвиток інформаційної безпеки як суспільного явища іноді знаходить своє відображення у нормативно-правових документах. Інформаційний складник національної безпеки розвивається у пришвидшеному темпі порівняно з іншими її складниками, що зумовлюється постійним впливом об'єктивних і суб'єктивних факторів.

Стан правового регулювання інформаційної безпеки в Україні залишається в не найкращому стані. Для вирішення особливо гострих питань у цій сфері необхідним є вироблення національних стратегічних пріоритетів та основних засад побудови та впровадження державної політики в інформаційній сфері. Згадані заходи у сукупності сформулюють нову парадигму кодифікації законодавства про інформацію. Досить важливою у такому процесі є роль інтелектуально-кадрового потенціалу, який має бути сформований за рахунок спеціалізованої підготовки фахівців у вищих навчальних закладах, зокрема у сфері права, адже такі фахівці на основі прогресивних наукових розроблень мають визначити шляхи вдосконалення вітчизняного інформаційного законодавства з урахуванням позитивних результатів інших держав.

Слушною є позиція П.С. Прибутька та І.Б. Лук'янцева, якими інформаційна безпека в умовах розвитку інформаційного суспільства визначається як рівень захищеності та стійкості основних джерел життєдіяльності від негативних інформаційних впливів [13, с. 210–211]. Але не зовсім погоджуємося з авторами щодо визначення інформаційної безпеки як рівня, вважаючи більш доцільним використання слова «стан». Частина дослідників також підтримує таку позицію [14, с. 296–297; 15, с. 109]. Під час визначення інформаційної безпеки важливим є врахування динамічних факторів розвитку суспільних відносин, що виступають об'єктом забезпечення безпеки.

Зазначимо, що вищезгадане розуміння інформаційної безпеки інформаційного суспільства визначається в конкретний момент часу, тобто у статичності. А безпека розвитку інформаційного суспільства визначається як постійний розвиток, тобто у динамічності. Статична інформаційна безпека визначає захист суспільних відносин від негативних інформаційних впливів, тому лишаються не включені певні елементи безпеки розвитку інформаційного суспільства, що знаходяться поза її межами. При цьому не враховуються функції у межах комунікацій, предметом яких є інформація. Беручи до уваги те, що комунікації здійснюються у всіх видах суспільних відносин, вважаємо, що саме безпека здійснення комунікацій виступає полем дії інформаційної безпеки. Визначаючи розвиток інформаційного суспільства, необхідно розуміти, що інформаційні процеси розвиваються у пришвидшеному темпі і є позитивною динамікою комунікацій людей у різних сферах життєдіяльності суспільства. Тобто важливим є створення безпечних умов для формування та розвитку комунікативних процесів у суспільстві, що є основою та найбільш сприятливим середовищем для розвитку інформаційного суспільства. Саме тому інформаційну безпеку доцільно також визначати станом організації та захищеності суспільних відносин, що здійснюються під час використання комунікацій.

Також важливою проблемою інформаційної безпеки є забезпечення захисту і контролю національного інформаційного простору, а також забезпечення інформації про державу у світовому інформаційному просторі. Під інформаційним простором розуміється певне середовище, у якому здійснюється формування, збирання, збереження, опрацювання і поширення інформації і на яке розповсюджується юрисдикція держави. Водночас інформаційне середовище, розуміється як сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням і споживанням інформації. Виділяють такі складники інформаційної безпеки: задоволення інформаційних потреб суб'єктів, включених в інформаційне середовище; забезпечення безпеки інформації; забезпечення захисту суб'єктів інформаційних відносин від негативного впливу [16, с. 56–57]. Інформаційне оснащення розвивається у пришвидшеному темпі. У результаті формується єдиний інформаційний простір, у якому відбуваються комунікації між суб'єктами інформаційних відносин. Бага-

то в чому життєдіяльність та оснащеність суспільства визначається рівнем розвитку та безпеки інформаційного середовища, що утворене у державі. Важливим також є рівень ефективності внутрішньодержавного нормативно-правового забезпечення, яким регулюється функціонування інформаційного простору. Інформаційне законодавство виражає прагнення керівництва держави до забезпечення допустимого чи бажаного рівня інформаційної безпеки та посилення впливу інформаційних технологій.

Вважаємо, що прогресивний розвиток та благополуччя суспільства всіляко сприяє усвідомленню населенням важливості захисту інформаційної безпеки, яка, як показують історичні приклади, є однією з найважливіших категорій розвитку людства, особливо із середини минулого століття. Саме тому інформаційна безпека має посісти важливе місце під час побудови майбутнього інформаційного суспільства. Ураховуючи динамічність цього явища, найбільш ефективним є інтегральний підхід, за якого інформаційна безпека буде досліджуватися на основі її основоположних ознак з урахуванням динамічного розвитку інформаційного простору. У цьому разі питання інформаційної безпеки можна розглядати більш комплексно і системно. Динамічність інформаційної безпеки визначає необхідність враховувати її не лише як стан, а і як процес. Помилковим є визначення інформаційної безпеки як ступеня захисту інформації. Уважаємо, що інформаційна безпека є багатоаспектним поняттям та, окрім вищезгаданого, може виступати багатогранною галуззю діяльності.

Визначальною характеристикою інформаційної безпеки є можливість виникнення непрогнозованих негативних погіршень стану життєдіяльності суспільства в інформаційній сфері, що призведуть до відповідних втрат та обмежень у подальшому розвитку.

До основних цілей забезпечення інформаційної безпеки належать такі: встановлення інформаційного суверенітету держави; організація державного інформаційного середовища; встановлення відповідного інформаційного простору; забезпечення захисту інформації від незаконних внутрішніх та зовнішніх посягань; створення умов для покращення ситуації в інформаційній сфері. Саме тому, з урахуванням зазначених вище факторів, державна політика у сфері інформаційної безпеки повинна реалізовуватись шляхом створення відповідної нормативно-правової бази у сфері регулювання інформаційної безпеки.

Як бачимо, проблематика правового забезпечення інформаційної безпеки держави становить перспективу для подальших наукових досліджень, що мають проводитися у сфері адміністративного та інформаційного права, а також безпекознавства, політології та інших наук. У цій проблематиці інституційно виділяються проблеми налагодження організаційного складника в системі державного управління в інформаційній сфері. Інформаційна безпека, як правове явище, визначається такими положеннями: формуванням загальних положень стосовно взаємовідносин у суспільстві; формуванням системних ознак організаційно-правових заходів; встановленням режиму охорони цінної для держави інформації від нерозповсюдження.

Багато у чому питання інформаційної безпеки у зовнішньому вимірі визначаються способами співіснування досліджуваної соціальної системи із іншими системами. Ними виступають державні або міждержавні структури. У внутрішньому вимірі ними виступають інтереси різних соціальних груп, які в сукупності складають таке суспільство. Ними можуть бути різні соціальні прошарки, партії чи організації. Сукупність внутрішніх і зовнішніх вимірів є важливою під час організації державного управління та забезпечення інформаційної безпеки відповідної держави. У результаті такої взаємодії забезпечується один із найважливіших елементів національної безпеки держави – інформаційна безпека.

Таким чином, держави, які не можуть забезпечити власну інформаційну безпеку, стають неконкурентоспроможними і, як наслідок, ризикують у недалекому майбутньому втратити свої переваги та зменшити свої темпи розвитку. Історія свідчить, що досить багато великих і успішних держав зникли через неможливість ефективно використовувати найновіші досягнення як у науково-технічному прогресі свого часу, так і в управлінні власною територіальною організацією. Щодо цього згадаємо, ситуацію початку позаминулого століття, коли для остаточної перемоги над Британською імперією Н. Бонапартіві потрібен був новий ефективний флот, але він не далекоглядно відкинув пропозицію Р. Фултона стосовно будівництва пароплавів, тобто кораблів, що могли рухатися без допомоги сили вітру. Тоді досить швидко досягненнями Р. Фултона скористались британці і на найближчі сто років жодна держава навіть не прагнула бути суперником британців у морі. Як бачимо, у будь-якій розвиненій державі має існувати система забезпечення інформаційної безпеки, а функції та повноваження відповідних державних органів повинні бути закріплені законодавчо. Аналіз вітчизняного законодавства показав, що до основних проблем за-

безпечення інформаційної безпеки належать проблеми загальносистемного характеру, пов'язані з відсутністю наукового обґрунтування і практичної апробації політики і методології інформаційної безпеки в контексті державної інформаційної політики.

Список використаних джерел:

1. Про телекомунікації / Закон України від 18 листопада 2003 р. № 1280-IV. // Відомості Верховної Ради України. – 2003. – № 12. – Ст. 155.
2. Про захист інформації в інформаційно-телекомунікаційних системах / Закон України від 31 травня 2005 р. № 2594-IV. // Відомості Верховної Ради України. – 2005. – № 26. – Ст. 347.
3. Про Концепцію Національної програми інформатизації / Закон України від 09 лютого 2006 р. № 3421-IV. // Відомості Верховної Ради України. – 2006. – № 22. – Ст. 199.
4. Про оборону України / Закон України від 11 травня 2007 р. № 1014-V. // Відомості Верховної Ради України. – 2007. – № 13. – Ст. 166.
5. Кравець Є.А. Інформаційна безпека держави. // Юридична енциклопедія. – 1992. – № 15. – С. 144–145.
6. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції [Текст] : навч. посіб. / В.А. Ліпкан, Ю.С. Макименко, В.М. Желіховський. – К. : КНТ, 2006. – 170 с.
7. Корнейко С. Застосування та визначення терміна «інформаційна безпека» в національному законодавстві. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2009. – № 2. – С. 9–13.
8. Про невідкладні заходи щодо забезпечення інформаційної безпеки України / Указ Президента України. / Режим доступу: <http://zakon3.rada.gov.ua/laws/show/n0010525-08> (втратив чинність).
9. Концепція національної інформаційної політики / Проект Закону. Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=13798.
10. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України / Указ Президента України. Режим доступу: www.president.gov.ua/dokument/17588.html.
11. Відбулось перше засідання Експертної Ради з розробки концепції інформаційної безпеки та з питань розвитку інформаційного простору. Режим доступу: www.kmu.gov.ua/kontral/uk/pullish/article.
12. Про інформаційний суверенітет та інформаційну безпеку України / Проект Закону України. Режим доступу: <http://www.rada.kiev.ua>.
13. Прибутко П.С. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах / П.С. Прибутко, І.Б. Лук'янець. – К., 2007. – 350с.
14. Кормич Б.А. Трансформація поняття та типології інформації в новому інформаційному законодавстві. // Актуальні проблеми публічного та приватного права. – 2012. – № 6. – С. 296–305.
15. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура і напрямки реалізації: Навчальний посібник / О.Г. Данільян, О.П. Дзьобань, М.І. Панов. – Харків, 2002. – 350 с.
16. Алексенцев А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. – 1999. – № 1. – С. 56–57.