duties prescribed by land legislation is the major reason of application of administrative influence, we need important scientific research in the field of regulation of administrative responsibility of the subjects of land use.

Different definitions of types of illegal behavior in land relations and legal responsibility provided by the rules of the Land Code of Ukraine and the availability of appropriate formulations of offenses in the articles of the Code of Ukraine on administrative offenses need to be brought into a single, coherent, internally and externally consistent system to eliminate contradictions and fill in the gaps of legal regulation, and, thus, improve the efficiency of the Institute of administrative responsibility of the subjects of land use. All these issues cause the relevance of this study.

This article examines the problem of the need to coordinate the provisions of land legislation of Ukraine and the Code of Ukraine on Administrative Offences regarding the liability of the subjects of land use.

It is emphasized on the urgency of establishing administrative liability for failure in state registration of the rights to land and submission of false information about it, timely payment of land tax, increase of soil fertility and storage of other useful properties of land.

Key words: *land use, administrative responsibility, the Land Code, sanctions.*

Стаття надійшла 23 січня 2015 р.

УДК 342+35.083

В. Й. Шишко

ДОСВІД США В РЕАЛІЗАЦІЇ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Досліджено актуальні питання реалізації адміністративно-правового забезпечення державної політики інформаційної безпеки в Сполучених Штатах Америки (далі США). Спираючись на події в США 11 вересня 2001 року доведено, що нині доволі виразно спостерігається поділ світу на країни інформаційно розвинені та нові, що розвиваються.

Акцентовано, що антитерористичні операції в США зумовили низку новітніх тенденцій у реалізації державної політики інформаційної безпеки, які спричинили переформатування внутрішніх і зовнішніх інформаційних потоків, запровадження нових механізмів адміністративно-правового регулювання

у сфері інформаційної безпеки, а також нових моделей комунікацій між владою, засобами масової інформації та масовою аудиторією. Відзначено, що нині США, як і більшість країн Заходу, зіткнулися з необхідністю удосконалення, з одного боку, функціонування державного апарату, а з іншого – за допомогою адміністративно-правових засобів забезпечення інформаційної безпеки.

Доведено, що забезпечення державою високого рівня інформаційної безпеки є умовою рівноправної участі у світових і цивілізаційних процесах. Тому нині нагальним є визначення ролі ІТ у сфері національних інтересів, виявлення загроз, оцінка їх рівня, формування ефективної державної системи управління ризиками із залученням громадськості та приватного сектора.

Ключові слова: *адміністративно-правове забезпечення, інформаційна безпека, інформаційні технології, адміністративно-правові засоби, комунікації, кіберзлочинність.*

Постановка проблеми. Невпинно накопичувати свої інформаційні ресурси й ефективно ними керувати – найважливіша проблема національної й міжнародної безпеки України. Це насамперед пов'язано з військовою агресією Росії проти України, а також із намаганням нашої країни бути повноправним учасником у системі координації глобального інформаційного суспільства.

Своєю чергою, необхідний аналіз і відповідний рівень формалізації та узагальнення досвіду, набутого «інформаційно розвиненими» країнами у сфері державного управлінні інформаційними потоками та інформаційними ресурсами за певних зовнішніх і внутрішніх кризових умов, а також реалізація адміністративно-правових засобів забезпечення інформаційної безпеки. Врахування вказаного є необхідним для забезпечення більш ефективної політики України у сфері захисту національного інформаційного простору.

Стан дослідження. Аналіз теоретичних джерел за значеною темою дослідження свідчить, що вивченню різних аспектів інформаційної безпеки приділяють значну увагу і вітчизняні, і зарубіжні дослідники. Серед зарубіжних учених вагомий внесок у розгляд цієї проблеми внесли С. Алексєєв, Л. Браун, Г. Кіссінджер, Ч. Флавін, Х. Френч. Серед вітчизняних дослідників слід відзначити праці В. Авер'янова, Ю. Битяка, Р. Калюжного, Т. Коломоєць, В. Колпакова, А. Комзюка, О. Кузьменко, В. Ліпкана, В. Лисюченка, А. Марущака, О. Остапенка, В. Петрика, О. Синявської, Л. Чистоклетова та інших науковців.

Незважаючи на актуальність, питання, пов'язані з аналізом зарубіжного досвіду щодо реалізації адміністративно-правових засобів

забезпечення інформаційної безпеки, не були предметом комплексного дослідження.

Метою статті є визначення шляхів наукової розробки окресленого напряму, які, на підставі досвіду правового інформаційного аналізув США, будуть спрямовані на вдосконалення комплексу адміністративно-правових засобів забезпечення інформаційної безпеки, напрацювання науково обґрунтованих пропозицій з цього питання та рекомендацій щодо правозастосовної практики у цій сфері.

Виклад основних положень. Генеральна Асамблея ООН виявляє глибоку занепокоєність диспропорціями між розвиненими країнами і країнами, що розвиваються. Адже це безпосередньо впливає на змогу останніх ефективно інтегруватись у світове співтовариство, відтак на їхню міжнародну конкурентоспроможність. Тому ООН на різних міжнародних форумах закликає до «нового міжнародного порядку в галузі інформації і комунікації», який розглядається як неперервний процес. Нині виникла нетривіальна ситуація підпорядкованості більшості аспектів розвитку будь-якої держави інтересам національної та міжнародної інформаційної безпеки, значущість яких переконливо довела ухвалена 23 липня 2000 р. Окінавська хартія глобального інформаційного суспільства.

Своєю чергою, це підтвердив Всесвітній саміт з інформаційного суспільства під егідою Організації Об'єднаних Націй (ООН), перший етап якого відбувся у грудні 2003 р. у Женеві, а другий – у листопаді 2005 р. у Тунісі. Подібні документи глобального змісту є переконливим доказом того, що невпинне накопичування своїх інформаційних ресурсів й ефективне керування ними є нині найважливішою проблемою національної й міжнародної безпеки в Україні.

Події 11 вересня 2001 року спонукали Сполучені Штати Америки та інші держави світу контролювати інформаційно-комунікативні технології й інформаційний обмін. Нині доволі виразно спостерігається поділ світу на інформаційно розвинені країни та ті, що розвиваються. Посилюється інформаційна нерівність, що адекватно відображають терміни «інформаційний імперіалізм» та «інформаційне гетто» тощо [1, с. 31].

Як відомо, Сполучені Штати Америки були однією з перших країн, які розпочали процес інформатизації. Інші промислово розвинені країни світу, зрозумівши перспективність і неминучість цього процесу, вельми швидко зорієнтувались і розпочали нарощувати темпи впровадження комп'ютерів і засобів телекомунікацій.

Авторитетний американський соціолог і футуролог Елвін Тофлер у праці «Третя хвиля», досліджуючи питання розвитку інформації та техніки і їх роль у соціальних перетвореннях, доводить теорію «інформаційного суспільства», яку можна вважати різновидом теорії постіндустріалізму, основи якої сформували американські соціологи З. Бжезинський та Д. Белл. Дослідники дають різні визначення інформаційного суспільства, але одностайні в головному: інформація в інформаційному суспільстві стає домінуючою цінністю; «генерування, обробка і передача інформації стали фундаментальними джерелами продуктивності і влади» [2, с. 4].

Американським компаніям та університетам належить більша частина світових патентів у сфері інформаційних технологій. У середині 1990-х років у США були зосереджені 426 із 816 світових інформаційних банків даних із науково-технічних дисциплін і 716 із 1035 наявних у світі баз даних із економічних дисциплін. Найближчими роками США залишаться найбільшим у світі ринком програмного забезпечення [3, с. 34].

У сучасному світі прогрес неможливий без цифрової інфраструктури – наріжний камінь процвітання економіки, сильної армії, відкритого й ефективного уряду. У реальності ми щодня залежимо від кіберпростору. Він охоплює все наше обладнання та програми, настільні й портативні комп'ютери, мобільні телефони, які вплетені в тканину кожного аспекту нашого повсякденного життя. Це широкосмугові та бездротові мережі, локальні мережі в школах, лікарнях, на підприємствах, інші масові мережі, які служать країні. Це і таємні військові і розвідувальні мережі, і відкритий web, який пов'язав людей сильніше, ніж будь-коли в історії людства.

США, як одна з найбільш інформаційно розвинутих країн, першими зіткнулися з проблемою забезпечення приватності особистого життя та економічної безпеки своїх громадян. Мільйони американців уже стали жертвами кіберзлочинців: їх приватне життя порушується, особисті дані викрадаються, гаманці спорожняються і життя перевертається догори дном. За даними дослідження групи «ЛЮ», тільки останніми двома роками кіберзлочинність коштувала американцям 8 млрд доларів [4, с. 16]. У серпні–жовтні 2008 року хакери отримали доступ до електронної пошти і низки файлів передвиборної кампанії Барака Обами, включаючи документи, що розкривають політичні позиції та плани поїздок. Штабістам довелося тісно співпрацювати з Центральним розвідувальним управлінням (ЦРУ), Федеральним

бюро розслідувань (ФБР) США, наймати консультантів для відновлення систем [4, с. 16]. За оцінками спеціалістів, упродовж одного року в усьому світі кіберзлочинці викрадають інтелектуальної власності в середньому на суму до $ 1 трлн [5]. Економічне процвітання Америки в XXI столітті залежатиме від кібербезпеки. Тепер очевидно, що кіберзагроза – це одна з найсерйозніших економічних і національних проблем цієї держави.

Нині Сполучені Штати Америки, як і більшість країн Заходу, зіткнулися з необхідністю удосконалення, з одного боку, функціонування державного апарату, а з іншого, – за допомогою адміністративно-правових засобів забезпечення інформаційної безпеки, що спричинено справжньою революцією у сфері комунікацій та інформаційних технологій, яка призвела до виникнення низки абсолютно нових неврегульованих правом суспільних відносин.

У травні 2009 року при федеральному уряді США була створена Єдина Рада з національної безпеки, однією з основних функцій якої є нагляд за реалізацією політики кібербезпеки. У Білому Домі створено також новий відділ, яким керує Координатор з кібербезпеки [6], який підпорядковується безпосередньо президенту. Слід підкреслити важливість функцій, які виконуються на цій посаді: це інтеграція і злагоджена робота всіх аспектів політики кібербезпеки в галузі управління; тісна співпраця з офісами Білого Дому, а також координація дій у відповідь у випадку надзвичайних подій або нападів. З метою посилення федерального складника політики зміцнення інформаційної безпеки Координатор з кібербезпеки також є членом Ради Національної безпеки, Національної економічної ради.

У доповіді від 29 травня 2009 року Б. Обама визначив п’ять головних напрямів діяльності, зокрема: розробка нової стратегії забезпечення безпеки інформаційно-комунікаційних мереж Америки; налагодження взаємодії державних і місцевих органів влади з метою забезпечення організованої відповіді на кібератаки; зміцнення співробітництва державного та приватного секторів; запровадження національної пропагандистської кампанії з метою поширення серед населення інформованості і грамотності у сфері цифрових технологій [7].

Про початок епохи «гонки озброєнь» у кіберпросторі оголосив голова компанії-розробника антивірусних програм McAfee Дейв ді Велт під час Всесвітнього економічного форуму в Давосі в січні 2010 року. За його словами, останнім часом спостерігається рух державних комп’ютерних структур від традиційних оборонних стратегій

до наступальних. Інтернет стає полем міжнародних бойових дій. Півтора-два десятки країн, серед яких Росія, США та Китай, готуються до можливих операцій в Інтернеті. Експерти закликають до активного публічного обговорення проблеми віртуальних воєн [8, с. 58].

Загалом останнім часом спостерігається різке збільшення кількості хакерських атак в усьому світі. Зокрема, за підрахунками McAfee, за рік кількість нових шкідливих програм зросла на 500%. Також фіксується підвищена увага світової громадськості до кібергалузі. Це наочно демонструє, на думку ді Велта, недавній випадок із компанією Google, яка після хакерської атаки на поштовий сервіс заявила про намір припинити роботу в Китаї. Експерти попереджають, що в майбутньому кібератаки проти ключових об'єктів життєзабезпечення, які в більшості розвинених країн недостатньо захищені, можуть обернутися величезною шкодою. Зараз, як довело дослідження McAfee, атаки хакерів обходяться в середньому в $ 6,3 млн. на добу, тобто в $ 1,75 млрд на рік у світі [9, с. 45].

Під час опитування 54% менеджерів вищої ланки визнали, що очолювані ними об'єкти постраждали від великомасштабних кібератак із боку організованих злочинців, терористів та окремих держав. Окрім того, 37% респондентів повідомили про те, що минулого року через скорочення корпоративних бюджетів ситуація з кібербезпекою погіршилася. Сорок відсотків опитаних очікують у новому році великого інциденту в сфері кібернетичної безпеки. Середня величина прогнозованої шкоди від «простою», спричиненої збоєм у роботі IT-систем, становитиме близько 6,3 мільйона доларів на день. 45% керівників уважають, що відповідальність за запобігання таким атакам повинні нести регіональні або місцеві органи влади [10, с. 27].

Щоб запобігти світовій кібервійні, експерти розглядають найбільш різноманітні варіанти контролю, зокрема в сфері адміністративно-правового регулювання. Так, Касперський запропонував заснувати Інтернет-поліцію. На Всесвітньому економічному форумі в Давосі генеральний секретар Міжнародного телекомунікаційного союзу Хамадун Туре наголосив, що сучасний світ має потребу в договорі, який міг би запобігти прийдешній світовій кібервійні. Директор із досліджень і стратегії корпорації Microsoft Крейг Манді як рішення запропонував ввести обов'язковий документ для Інтернет-користувачів – аналог водійських прав. «Проблема в тому, що люди не розуміють масштаби і загрозу злочинної діяльності в Інтернеті», – заявив він [11, с. 63].

Адміністрація Барака Обами заявила, що здійснюватиме новий комплексний підхід до забезпечення безпеки цифрової інфраструктури Америки.

Надалі американська цифрова інфраструктура – мережі та комп'ютери – розглядатимуться як стратегічний національний актив. Захист цієї інфраструктури, зокрема адміністративно-правовими засобами, буде пріоритетом національної безпеки.

Отже, впровадження нової стратегії інформаційної безпеки Бараком Обамою у США свідчить про зростаючу роль впливу цієї сфери людської діяльності на забезпечення стабільного функціонування державного апарату в одній з найбільших країн світу.

В сучасних умовах у складі національної безпеки питома вага інформаційної безпеки зростає завдяки розширенню застосування і збільшенню вразливості інформаційних технологій у критичних галузях (енергетика, транспорт, трубопроводи, промисловість, фінанси тощо). У зв'язку з цим у світову практику впроваджено поняття критичної інформаційної інфраструктури, англомовний аналог «Critical Information Infrastructure» (CII), а процес її захисту – «Critical Information Infrastructure Protection» (CIIP) [12].

Належну увагу захисту критичної інфраструктури приділяє НАТО. Так, Комітет планування надзвичайних дій у цивільному секторі (Senior Civil Emergency Planning Committee – SCEPC) визначає шляхи допомоги державам у підготовці захисту громадян від терористичних нападів на критичну інфраструктуру. Плановий комітет цивільних комунікацій (CCPC) відповідає за планування захисту суспільних і спеціальних інформаційних систем, з огляду на рівень розвитку технологій, національне законодавство, міжнародні домовленості та стандарти.

Висновки. Вивчення американського досвіду у сфері реалізації адміністративно-правового забезпечення державної політики інформаційної безпеки свідчить про те, що нині однією з найважливіших проблем інформаційно розвинутих держав є те, що впровадження інформаційних технологій відбувається швидше, ніж процеси правового регулювання пов'язаних із цим суспільних відносин.

З уваги на досвід США, вітчизняні органи державної влади повинні взяти під регулюючий контроль побудову національної інформаційної інфраструктури. Ситуація ускладнюється ще і тим, що впровадження ІТ в нашій державі супроводжується залежністю від їхньої захищеності. Ключові програмно-апаратні засоби інформаційно-

комунікаційних систем розробляються за межами України, тому наша країна позбавлена можливості доступу до їх технічних характеристик. Водночас у розвинутих країнах розробники інформаційних систем активно співпрацюють із урядовими структурами у питаннях забезпечення національної безпеки.

Забезпечення державою високого рівня інформаційної безпеки є умовою рівноправної участі у світових і цивілізаційних процесах. Тому нині нагальним є визначення ролі ІТ у сфері національних інтересів, виявлення загроз, оцінка їх рівня, формування ефективної державної системи управління ризиками із залученням громадськості та приватного сектора.

1. Інформаційні технології та тенденції розвитку міжнародної інформації // Вісник книжкової палати. – 2010. – № 6. – С. 30–32.

2. Кастельс Мануель. Информационная эпоха: экономика, общество и культура / Мануель Кастельс; пер. с англ., под науч. ред. О. И. Шкаратана. – М., 2000. – С. 4.

3. Роговской Е. Развитие информационного сектора США к началу XXI века / Е. Роговский. – США–Канада. – 2002. – № 4. – С. 32–37.

4. AIG Technology Report 2007–2008: Readiness for the Networked World Center for International Development at Harvard University, March 2009. – P. 14–18.

5. WIPO 2008 Report / WIPO Site. [Електронний ресурс]. – Режим доступу: http://www.wipo.int/meetings/en/archive.jsp.

6. Barack Obama Speech, March, 13, 2009 / Barack Obama Site. [Електронний ресурс]. – Режим доступу: http://my.barackobama.com/page/content/ofasplashbsignon/.

7. Remarks by the President on Securing our Nation's Cyber Infrastructure // White House Official Site. [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/the_pressoffice/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

8. Тумарец В. Новые угрозы для информационного общества / В. Тумарец. – М.: ЭКСМО, 2008. – 288 с.

9. Прохожев А. А. Основы информационной войны. Анализ систем на пороге XXI века: теория и практика / А. А. Прохожев, Н. И. Турко. – М., 1996. – 388 с.

10. Даниелова А. Основные направления информатизации американского общества / А. Даниелова // США–Канада. – 2009. – № 5. – С. 25–29.

11. Шершнёв Е. Информатизация общества и экономики США / Е. Шершнёв // США–Канада. – 2008. – № 1. – С. 61–65.

12. Critical Infrastructure Protection Study. // White House Symantec 2010. [Електронний ресурс]. – Режим доступу: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=CIP_survey

Шишко В. И. Опыт США в реализации административно-правового обеспечения государственной политики информационной безопасности

Исследуются актуальные вопросы реализации административно-правового обеспечения государственной политики информационной безопасности в Соединенных Штатах Америки.

Доказывается, что в настоящее время достаточно отчетливо наблюдается разделение мира на информационно развитые и новые развивающиеся страны. Акцентируется, что антитеррористические операции в США обусловили ряд новейших тенденций в реализации государственной политики информационной безопасности, повлекших переформатирование внутренних и внешних информационных потоков, внедрение новых механизмов административно-правового регулирования в сфере информационной безопасности, а также новых моделей коммуникаций между властью, средствами массовой информации и массовой аудиторией.

Отмечается, что в настоящее время США, как и большинство стран Запада, столкнулись с необходимостью усовершенствования, с одной стороны, функционирования государственного аппарата, а с другой – с помощью административно-правовых средств обеспечения информационной безопасности. Доказывается, что обеспечение государством высокого уровня информационной безопасности является условием равноправного участия в мировых и цивилизационных процессах.

Ключевые слова: *административно-правовое обеспечение, информационная безопасность, информационные технологии, административно-правовые средства, коммуникации, киберпреступность.*

Shishko V. I. The USA experience of realizing the administrative-legal support of information security state policy

The article considers the problems of administrative-legal support of state information security policy in the USA.

The theoretical and practical study of unconventional situation of subordinating the aspects of the interests of national and international security have been analyzed based on Okinawan Charter on Global Information Society and the World Summit on the Information Society under the auspices of the UN.

On the basis of the events in the USA on September, 11, 2001, it is proved that there is a distinct division between informative-developed countries and the ones to be developed.

The article emphasizes that the antiterrorist operation in the USA resulted in a number of recent trends in the state security policy which led to reformatting the

internal and external information flows, forming new mechanisms and administrative-legal regulation in the field of information security and developing new models of communication between the government, media and mass audience.

It is noted that nowadays the USA and most Western countries have faced the necessity to improve the functioning of the state apparatus, on the one hand, and using the legal and administrative means of information security, on the other hand. This fact caused a real revolution in communications and information technology, which leads to arising a number of absolutely new social relations non-regulated by law.

It is proved that information security of high level provided by the state is a necessary condition of equal participation in the world and civilized processes. So, it is now urgent and important to determine the role of IT in the national interest, to determine possible threads, to evaluate their level and to form the effective state system of risk regulation managed by the public and private sector.

Key words: *administrative and legal security, information security, information technology, administrative and legal means of communication, cybercrime.*

Стаття надійшла 12 січня 2015 р.