УДК 342.345.54

Ю. П. ЛІСОВСЬКА
Міжрегіональна Академія управління персоналом, м. Київ

КОНЦЕПЦІЯ ПРЕВЕНТИВНИХ ЗАХОДІВ У СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: АДМІНІСТРАТИВНО-ПРАВОВИЙ АСПЕКТ

Наукові праці МАУП, 2017, вип. 52(1), с. 103–109

Розглядаються основні шляхи і напрями реалізації концептуальних положень інформаційної безпеки держави в науково обґрунтованій концепції превентивних заходів у системі інформаційної безпеки.

Для ефективного забезпечення інформаційної безпеки на рівні особи, держави та суспільства кожній країні необхідно розробити ідеологічну основу для цього. Таким чином, формується єдине розуміння організації діяльності суб'єктів забезпечення інформаційної безпеки, нормативно-правова основа, яка визначає спектр їхніх прав та обов'язків, а також створює єдину державну політику адміністративно-правового забезпечення інформаційної безпеки в Україні. Система забезпечення інформаційної безпеки має включати комплекс превентивних заходів з надання гарантій захисту життєво важливих інтересів особи, держави, суспільства, своєчасного і адекватного реагування на весь спектр інформаційних безпекогенних чинників з метою захисту національних інтересів та національної безпеки.

Питання інформаційної безпеки стало предметом наукових дискусій у межах робіт таких вчених, як І. Арістова, І. Березовська, В. Голубєв, В. Гурковський, О. Дзьобань, Р. Калюжний, В. Конах, Б. Кормич, В. Ліпкан, Ю. Максименко, А. Марущак, В. Цимбалюк, О. Юдін, Р. Юсупов та ін. Однак вивченню сьогоденної концепції інформаційної безпеки України не приділялося уваги вітчизняними дослідниками. Тож можна виокремити такі ключові напрями концепції превентивних заходів у системі інформаційної безпеки України.

Першим напрямом концепції превентивних заходів у системі інформаційної безпеки має стати формування державної політики інформаційної безпеки з відповідними органами. При цьому мають враховувати усі рекомендації міжнародних інституцій та створюватися належна нормативно-правова база. Наразі до такої системи належать:

- Конституція України;
- Закони України "Про основи національної безпеки України", "Про інформацію", "Про Основні засади розвитку інформаційного суспільства в

Україні на 2007–2015 роки", "Про Концепцію Національної програми інформатизації", "Про Національну програму інформатизації", "Про державну таємницю", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про внесення змін до Закону України "Про ратифікацію Конвенції про кіберзлочинність", "Про доступ до публічної інформації", "Про Раду національної безпеки і оборони", "Про боротьбу з тероризмом", Цивільний кодекс, Кримінальний кодекс, Кодекс України про адміністративні правопорушення;

• Укази Президента України "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України", "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України", "Про заходи щодо захисту інформаційних ресурсів держави", "Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України";

• Постанови Кабінету Міністрів України "Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах", "Питання Адміністрації Державної служби спеціального зв'язку та захисту інформації";

• Розпорядження Кабінету Міністрів України "Про схвалення Концепції розвитку електронного урядування у Україні", "Питання впровадження системи електронної взаємодії органів виконавчої влади".

Другим напрямом концепції превентивних заходів у системі інформаційної безпеки України є удосконалення адміністративно-деліктного законодавства у сфері інформаційної безпеки України:

– виокремлення в межах КУпАП окремого розділу, об'єктом адмінправопорушень яких є інформаційна безпека людини (особи, громадянина), держави та суспільства. Під час розгляду складу кожного з правопорушень у сфері інформаційної безпеки, що передбачені КУпАП, виникають певні труднощі, тому що чинний КУпАП не має окремої глави, присвяченій саме правопорушенням в інформаційній сфері, а правопорушення, які можна віднести до інформаційної безпеки, розташовані у різних главах Особливої частини КУпАП;

– у законодавстві з'являються норми, які передбачають накладення стягнень на юридичних осіб, зокрема, за правопорушення у сфері інформаційної безпеки. За вчинення адміністративного порушення у сфері інформаційної безпеки на фізичних осіб найчастіше накладається штраф. До цього виду адміністративної відповідальності також варто притягати і юридичних осіб — порушників законодавства. Враховуючи викладене, необхідно передбачити у чинному КУпАП розділ, який би містив перелік проступків в інформаційній сфері, а також закріпити у чинному КУпАП норми, які б передбачали адміністративну відповідальність юридичних осіб;

– посилення адмінвідповідальності за правопорушення інформаційного характеру;

– доповнення КУпАП статтею, що передбачає відповідальність за курси нейролінгвістичного програмування (НЛП), що завдають шкоду психіці людини;

– доповнення КУпАП нормою, що закріплює відповідальність за порушення правил збирання, розголошення та використання комерційної таємниці;

– доповнити Кодекс України про адміністративні правопорушення відповідальністю за невиконання законних вимог посадових осіб Служби безпеки України;

– у Закон України "Про основи національної безпеки України" внести зміни до визначення терміна "національна безпека";

– статтю 7 Закону України "Про основи національної безпеки України" доповнити переліком обставин, що можуть вважатися загрозою національній безпеці;

– статтю 8 Закону України "Про основи національної безпеки України" доповнити основними напрямами державної політики з питань національної безпеки в інформаційній сфері.

Третім напрямом концепції превентивних заходів у системі інформаційної безпеки є створення спеціалізованої служби, основним завданням якої б стало забезпечення координації дій всіх державних та недержавних інституцій у сфері забезпечення інформаційної безпеки України. Доречно зауважити, що при Міністерстві інформаційної політики України створено Експертну раду згідно з Положенням "Про Експертну раду при Міністерстві інформаційної політики України" як дорадчий орган, що має своєю метою забезпечення взаємодії з науково-дослідними установами, неурядовими аналітичними центрами, інститутами громадянського суспільства, іншими вітчизняними та зарубіжними організаціями [1].

Четвертий напрям концепції превентивних заходів у системі інформаційної безпеки полягає в ефективному, якісному реформуванні законодавства, що стосується інформаційної безпеки. Водночас, розглядаючи адміністративно-правове регулювання інформаційної сфери як основу забезпечення інформаційної безпеки держави, слід зазначити, що упродовж останніх років законодавча база України в інформаційній сфері поповнилася низкою законів, з-поміж яких надзвичайно важливими є Закони України "Про інформацію", "Про державну таємницю", "Про захист інформації в автоматизованих системах", "Про науково-технічну інформацію", "Про систему іномовлення України", останній з яких Верховна Рада ухвалила 8 грудня 2015 р. тощо.

Члени робочої групи при парламентському Комітеті з питань свободи слова та інформаційної політики, до якої входять народні депутати, представники громадських організацій та медіаіндустрії, обговорили проект Стратегії розвитку законодавства України з питань свободи слова та діяльності ЗМІ відповідно до європейських стандартів, який розроблено за підтримки спільної програми ЄС та РЄ "Зміцнення інформаційного суспільства в Україні".

Нова редакція Закону України "Про суспільне телебачення і радіомовлення України" дала можливість запустити одну з найважливіших медіареформ: перетворення державного мовлення на суспільне. Закон України "Про реформування державних і комунальних друкованих засобів масової інформації", до якого країна йшла багато років, передбачає приватизацію державних і

комунальних друкованих видань у два етапи: спершу один рік — добровільно для охочих редакцій, наступні два роки — роздержавлення решти видань.

Закон України "Про внесення змін до деяких законодавчих актів України (щодо особливостей трансляції (ретрансляції) реклами, яка міститься у програмах та передачах іноземних телерадіоорганізацій)" заборонив транслювати рекламу на російських каналах в Україні та узаконив так званий список адаптованих каналів, що складає Національна рада з питань телебачення і радіомовлення. Діє Постанова "Про тимчасове призупинення акредитації журналістів та технічних працівників деяких засобів масової інформації Російської Федерації при органах державної влади України". Закон України "Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації та реалізації принципів державної політики у сфері телебачення і радіомовлення" набув чинності 1 жовтня 2015 р., його основною метою є відкриття даних про кінцевих власників та структуру власності телерадіоорганізацій і провайдерів програмної послуги.

Створення національної правової бази, гармонізованої з міжнародними інституціями, сприятиме зміцненню інформаційної безпеки України та підвищенню її міжнародного авторитету як демократичної і правової держави. Створення національної правової бази має передбачати:

1) Концепцію національної інформаційної політики України та Інформаційний кодекс України як базовий нормативний акт;

2) включення до Стратегії національної безпеки України спеціального розділу "Стан інформаційної безпеки України", в якому слід чітко визначити актуальні проблеми державної політики забезпечення інформаційної безпеки та зосередити увагу на необхідності їх вирішення;

3) створення єдиного державного реєстру власників ЗМІ;

4) постійний розвиток індустрії інформаційних послуг та інфраструктур інформаційного простору України.

П'ятим напрямом концепції превентивних заходів у системі інформаційної безпеки є забезпечення програм відкритого доступу до публічної інформації та створення ефективних умов щодо її отримання.

За роки членства України в Раді Європи поступово складаються механізми залучення громадськості до напрацювання та здійснення відкритої та прозорої державної політики. Наукові дослідження таких механізмів могли б сприяти оптимізації цих процесів, однак у науковій літературі не спостерігається інтересу до цієї проблеми.

Система зв'язків з громадськістю фінансується з державних бюджетів, але у проектах Державного бюджету України не було закладено коштів на фінансування таких зв'язків, які могли б сприяти публічному дослідженню, зокрема, якості врахування пропозицій громадян [2, *40*].

Україна приєдналася до Декларації Відкритого Уряду, що передбачає розширення відкритої інформації для залучення громадян у процеси прийняття рішень, стимулювання доброчесної поведінки державних службовців [3].

Забезпечення реалізації Ініціативи "ПВУ" у 2014–2015 рр. покладено на Кабінет Міністрів України, одним із напрямів якої є забезпечення доступу

до публічної інформації. З 6 взятих зобов'язань за 2 роки було виконано лише 3 пункти [3].

Проектом прийнятої у 2015 р. Національної стратегії у сфері прав людини передбачалось вирішити деякі з проблем шляхом запровадження механізму реалізації права на доступ до публічної інформації та забезпечивши певні гарантії доступу громадськості до необхідних Інтернет-ресурсів [4]. Проект концепції інформаційної безпеки України [5] став об'єктом критики громадськості через ряд серйозних недоліків [6].

Закон України "Про внесення змін до статті 28 Бюджетного кодексу України щодо доступу до інформації про бюджетні показники у формі відкритих даних" зобов'язує оприлюднювати матеріали квартальної та річної звітності з виконання Державного бюджету України, бюджетних запитів, паспортів бюджетних програм та звітів про їх виконання, інформації про місцеві бюджети.

Шостим напрямом концепції превентивних заходів у системі інформаційної безпеки вбачається реформування наявної системи електронного урядування.

Сьогодні проявом оптимізації взаємодії індивідів та держави на новому рівні є спроба впровадження програм електронного уряду, покликаних сприяти зменшенню бюрократичності, збільшенню відкритості і прозорості діяльності органів управління та поступовому відходу від тотального використання паперової технології. У вітчизняній науковій літературі дослідженню проблематики електронного урядування, його характеристик та стану впровадження у практичну діяльність органів влади присвячено праці таких провідних науковців, як Д. Дубов, С. Дубова, І. Клименко, С. Кузнєцова, К. Линьова, О. Мітченко, З. Пісковець, О. Рискова, В. Шеверда, О. Юлдашев та ін.

В Україні діє Концепція розвитку електронного урядування, затверджена Розпорядженням КМУ від 13 грудня 2010 р., у якій сформовані основні принципи та прогнози щодо запровадження електронного урядування в державних органах влади та органах місцевого самоврядування.

До основних завдань електронного уряду відносять: "організацію державного управління на основі електронних засобів обробки, передачі та розповсюдження інформації; надання послуг державних органів всіх гілок влади всім категоріям громадян (пенсіонерам, робітникам, бізнесменам, державним службовцям тощо) електронними засобами; інформування тими ж засобами громадян про роботу державних органів" [8].

Сьомим напрямом концепції превентивних заходів у системі інформаційної безпеки має стати системно-аналітична розробка цілісної теорії загроз. Розглядаючи поняття "інформаційна безпека" через захищеність від небезпек та загроз, виникає проблема розробки цілісної теорії загроз, оскільки немає єдиної методології у визначенні загроз, у їх співвідношенні між собою. Раніше загрози мали зовнішній та воєнний характер, коли невоєнні та воєнні засоби практично неможливо було використовувати комплексно, але зараз в умовах взаємозалежності світу та нових технологій загрози носять, як правило, комплексний характер [9, *39*].

Слабкість інформаційної інфраструктури дозволяє іноземним компаніям проводити експансію на ринку інформаційних послуг, що веде до перероз-

поділу ефірного часу на користь іноземних економічних та політичних бенефіціарів [10, *17*].

"Загрози" в інформаційній безпеці виглядають як сукупність умов та факторів, які становлять небезпеку життєво важливим інтересам особи, держави та суспільства у зв'язку з можливістю негативно впливати на свідомість і поведінку громадян, а також на інформаційно-комунікаційну інфраструктуру.

Унікальною особливістю інформаційної загрози є те, що вона виступає як самостійна загроза і водночас є основою для інших видів загроз на інформаційному рівні, у тому числі і їх першопричиною.

Таким чином, сьогодні не існує достатніх гарантій захисту особи від загроз, пов'язаних з порушенням інформаційної безпеки особи. Тому виникла значною мірою соціальна небезпека безконтрольного застосування технологій, засобів і методів психофізичного впливу на певні соціальні групи людей через свідомість і підсвідомість людини з метою формування необхідних подій та маніпулювання громадською думкою. Інформаційна безпека особи й суспільства є складовою інформаційної безпеки держави: її забезпечення посідає особливе місце в державній політиці. Ця особливість визначається специфікою загроз та їх джерел. Найважливішими об'єктами захисту в сучасних умовах є індивідуальна та масова свідомість. Руйнація свідомості небезпечніше руйнації в економіці, тому що втрата національних, духовних цінностей призводить до виродження народу і краху суспільства.

Джерела

1. Положення про Спеціалізовані експертні ради при Міністерстві інформаційної політики України [Електронний ресурс] // Ukraina haber siyaseti nazirligi. URL: http://mip.gov.ua/cr/documents/14.html
2. Основні засади діяльності прес-служб органів державної влади та місцевого самоврядування: світовий та український досвід: довідник. Донецьк: ДонДУ, 2011. 96 с.
3. "Відкритий уряд" в Україні: Перезавантаження // Transparency International Україна. URL: http://ti-ukraine.org/news/oficial/5308.html
4. Національна стратегія у сфері прав людини (проект, станом на 25 березня 2015 року) // Міністерство юстиції. URL: http://old.minjust.gov.ua/file/44709
5. В Україні найближчим часом з'явиться доктрина інформаційної безпеки // Видання Міністерства оборони України "Народна армія". 2015. Жовтень 27. URL: http://na.mil.gov.ua/25677-v-ukra%D1%97ni-najblizhchim-chasom-zyavitsya-doktrina-informacijno%D1%97-bezpeki
6. *Шутов Р.* Глиняний фундамент інформаційної безпеки [Електронний ресурс] // MediaSapiens. URL: http://osvita.mediasapiens.ua/media_law/law/koli_sosud_napiv-porozhniy_scho_robiti_z_kontseptsieyu_informatsiynoi_bezpeki/
7. Парламент ухвалив два закони щодо доступу до відкритих даних // Телекритика. URL: http://www.telekritika.ua/pravo/2015-04-09/105929
8. *Голобуцький О., Шевчук О.* "Електронний уряд" [Електронний ресурс] // URL: http://golob.narod.ru/egovper.html
9. *Лопатин В. Н.* Вопросы военной реформы и национальной безопасности России // Вестник Межпарламенской Ассамблеи СНГ. СПб., 1996. № 2. С. 38–42.
10. Інформаційна безпека держави: підручник / В. М. Петрик та ін.; за заг. ред. В. В. Остроухова; в 2 т. К.: ДНУ "Книжкова палата України", 2016. Т. 2. 328 с.

Для ефективного забезпечення інформаційної безпеки на рівні особи, держави та суспільства кожній країні необхідно розробити ідеологічну основу для цього. Таким чином, формується єдине розуміння організації діяльності суб'єктів забезпечення інформаційної безпеки, нормативно-правова основа, яка визначає спектр їхніх прав та обов'язків, а також створює єдину державну політику адміністративно-правового забезпечення інформаційної безпеки в Україні.

"Threats" in information security look like a set of conditions and factors that pose a threat to the vital interests of the person the state and society in relation to the possibility of a negative impact on public consciousness and behavior, as well as information and communication infrastructure. A unique feature of threat information is that it acts as an independent threat and is also the basis for other types of threats on the information level, including their root cause. Thus, today there are no sufficient guarantees protection of persons against threats related to violation of information security person. Therefore, there largely social danger of uncontrolled use of technologies, tools and methods psychophysical effects on certain social groups of people through human consciousness and subconscious in order to create the necessary events and manipulate public opinion. Information security of the individual and society is part of information security, ensuring it has a special place in public policy. This feature is determined by the specific threats and their sources. The most important objects of protection under current conditions is individual and mass consciousness. The destruction of consciousness dangerous destruction of the economy, so that the loss of national and spiritual values leads to degeneration of the people and the collapse of society. Effective information security at individual, state and society every country needs to develop an ideological basis for this. Thus, a common understanding of the organization of information security, regulatory and legal framework that defines the range of their rights and responsibilities, and creates a unified state policy of administrative and legal information security in Ukraine.

Для эффективного обеспечения информационной безопасности на уровне личности, государства и общества каждой стране необходимо разработать идеологическую основу для этого. Таким образом, формируется единое понимание организации деятельности субъектов обеспечения информационной безопасности, нормативно-правовая основа, которая определяет спектр их прав и обязанностей, а также создает единую государственную политику административно-правового обеспечения информационной безопасности в Украине.

Надійшла 3 лютого 2017 р.