УДК 355.405.1

Н. Б. Мєзєнцева,
кандидат наук з державного управління,
старший науковий співробітник військової частини А1906

ДО ПИТАННЯ НАУКОВОГО ОБГРУНТУВАННЯ ПОЛІТИКИ І МЕТОДОЛОГІЇ ДЕРЖАВНОЇ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

TO QUESTION THE SCIENTIFIC BASIS AND METHODOLOGY OF PUBLIC POLICY INFORMATION SECURITY SYSTEM

У статті розглядаються проблеми наукового обгрунтування і практичної апробації політики і методології державної системи інформаційної безпеки. Досліджуються питання систематизації, удосконалення та подальшого розвитку законодавства України за окремими функціональними сегментами інформаційної сфери в умовах інформаційної глобалізації.

In the article role of the problems of scientific studies and practical testing policy and methodology of the state of information security. The problems of organizing, improvement and further development of the law of Ukraine on individual functional segments of the information field in terms of information globalization.

Ключові слова: захист даних, інформаційна безпека, інформація, об'єкти, загрози.
Key words: data protection, information security, information, objects, threats.

ВСТУП

Інформаційна безпека є складовою загальної безпеки і стрімко розвивається як у всьому світі, так і в Україні, глобальна інформатизація охоплює всі сфери держави — економічну, військову, політичну, промислову і т.п. Інформаційна безпека, як і будь-який інший об'єкт, має загрози, які посягають як на цілісність фізичну, так і її похідних.

Історично інформація завжди мала величезне значення в побуті людей і завжди їй відводилося особливе місце, багато уваги приділялося розвитку засобів і методів її захисту.

Сьогоднішні умови політичного і соціально-економічного розвитку країни викликають загострення протиріч між потребами суспільства в розширенні вільного обміну інформацією і необхідністю збереження окремих обмежень на її поширення. Відсутність дієвих механізмів регулювання інформаційних відносин у суспільстві та державі призводить до багатьох негативних наслідків.

Метою даної статті є аналіз стану інформаційної безпеки України та виявлення основних проблем її забезпечення для наукового обгрунтування удосконалення і подальшого розвитку законодавства нашої держави в інформаційній сфері, політики і методології державної системи інформаційної безпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Актуальність статті зумовлена новими небезпеками, загрозами, викликами й ризиками сучасного світу. Про проблеми інформаційної складової, що виникають в умовах глобальної світової інтеграції і призводять до жорсткої міжнародної конкуренції в інформаційному просторі пишуть багато вітчизняних і зарубіжних дослідників — С. Антимонов, О. Власюк, В. Гавловський, В. Горбулін, В. Гурковський, В. Ліпкон, О. Логінов, О. Панарін, Г. Ситник, Д. Хеллі та ін. Геополітичні аспекти нових загроз досліджують З. Бауман, З. Бжезинський, С. Караганов, Е. Тофлер та інші дослідники.

Аналіз стану інформаційної безпеки України показує, що до основних проблем забезпечення інформаційної безпеки належать проблеми загальносистемного характеру, пов'язані з відсутністю наукового обгрунтування і практичної апробації політики і методології державної системи інформаційної безпеки. За характером це правові та нормативно-правові, науково-технічні, економічні, організаційні, кадрові проблеми тощо.

З метою запобігання, парирування і нейтралізації загроз інформаційної безпеки застосовуються базові методи. До них відносяться правові, програмно-технічні та організаційно-економічні методи.

Правові методи передбачають розробку комплексу нормативно-правових актів та положень, що регламентують інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо забезпечення інформаційної безпеки.

Пріоритетним завданням є створення законодавчої і нормативно-правової бази забезпечення інформаційної безпеки, а саме нормативно-правової бази щодо розподілу і використання персональної інформації з метою створення умов для інформаційних стосунків між органами державної влади і суспільства, формування передумов досягнення соціального компромісу, створення умов становлення соціального партнерства

як основи демократичного розвитку суспільства, розробки регламенту інформаційного обміну для органів державної влади і управління, реєстру інформаційних ресурсів, закріплення відповідальності посадових осіб, громадян за додержання вимог інформаційної безпеки.

Як відомо, інформаційна безпека, захист якої згідно ст. 117 Конституції України, поряд із суверенітетом, територіальною цілісністю та економічною безпекою, є найважливішою функцією держави, досягається шляхом розробки та впровадження сучасних безпечних інформаційних технологій, побудовою функціонально повної національної інфраструктури, формуванням і розвитком інформаційних відносин тощо.

Таким чином, можна стверджувати, що інформаційна безпека визначається здатністю держави, суспільства, особистості, по-перше, забезпечувати достатні і захищені інформаційні ресурси та інформаційні потоки для підтримки своєї життєдіяльності і життєздатності, стійкого функціонування і розвитку. По-друге, протистояти інформаційним небезпекам і загрозам, негативним інформаційним впливам на індивідуальну і суспільну свідомість і психіку людей, а також на комп'ютерні мережі та інші технічні джерела інформації. По-третє, виробляти особистісні й групові навички та вміння безпечної поведінки. І головне: підтримувати постійну готовність до адекватних заходів у інформаційному протиборстві, ким би воно не було нав'язано.

Серед основних геополітичних змін в інформаційній сфері, котрі відбулися на початку XXI століття, можна зафіксувати наступні:

— інформаційний простір західних держав стрімко перетворюється в єдиний глобальний інформаційний простір, де домінуючу роль у контролі над інформаційними потоками відіграють США і ЄС;

— формується глобальна інформаційна інфраструктура на основі мережі Інтернет та посилюється просторова взаємозалежність країн;

— істотно розширився військово-інформаційний простір, що контролюється державами-членами НАТО;

— у глобальному інформаційному просторі посилюються процеси, пов'язані з розвитком відносин партнерства і суперництва;

— однією з основних сфер геополітичного протиборства стає інформаційний простір глобального, регіонального і національного рівнів.

За довгостроковими прогнозами експертів, перспективи світового розвитку визначатиме глобальне перегрупування сил внаслідок інформаційного прогресу в США, ЄС, Японії, Китаї, Індії та Росії.

Крім того, на думку автора, передбачається розвиток трьох геостратегічних та інформаційних Центрів світу, перш за все, американського під егідою США, Європейського (ЄС) та азійського (Китай, Індія, Японія).

Останнім часом Російська Федерація також намагається стати одним з інформаційних Центрів світу та здійснює активний інформаційний вплив на пострадянському просторі [6].

Україна в такій міжнародній конструкції посідає особливе місце завдяки своєму геополітичному розташуванню.

Історичний досвід свідчить, що країни, які не спромоглися своєчасно поповнити національний інформаційний простір більш ефективними технологіями, сповільнювали свій економічний розвиток. І навпаки, країни, що мали потужний інформаційний потенціал, швидко відновлювали свою роль у світовому розподілі сфер впливу навіть після воєнних поразок. Тому наповнення національного інформаційного простору новітніми технологіями, що здатні істотно підвищити як адекватність відображення реальності, так і продуктивність інформаційної діяльності в суспільстві, є нагальною потребою, що у свою чергу визначає можливості захисту національних інтересів.

Ключові проблеми інформаційної безпеки обумовлені наступними факторами розвитку інформаційної сфери:

— стрімке формування глобального інформаційного простору та революційні зміни в інформаційній сфері активізують нові глобальні виклики і загрози;

— більшість країн світу вже зіштовхнулася з проблемами кібертероризму, кіберзлочинності та іншими проблемами інформаційної безпеки;

— протягом останніх десятиліть спостерігається тенденція до поширення інформаційної агресії і насилля;

— набувають поширення агресивна реклама, спроби маніпуляції свідомістю людини, періодично проводяться інформаційно-психологічні операції;

— майже у 120 країнах світу ведуться розробки інформаційної зброї або її елементів (розробки зброї масового знищення — у близько 20 країнах);

— наслідки використання сучасної інформаційної зброї є співставними із застосуванням зброї масового ураження;

— новітні виклики і загрози в інформаційній сфері становлять реальну загрозу безпеці людства та міжнародному правопорядку;

— жодна держава світу в умовах інформаційної глобалізації не здатна самостійно забезпечити власну інформаційну безпеку.

Серед системних проблем інформаційного виміру, які потребують наукового і правового опрацювання на рівні колективної безпеки, в першу чергу, потрібно розглянути перегляд принципів і механізмів міжнародних відносин та співробітництва в галузі інформаційної безпеки [3]. Існує необхідність міжнародно-правового визначення ключових понять в інформаційній сфері (у т.ч. розмежування понять "інформаційна безпека", "кібербезпека", "кіберзлочинність", "кібертероризм", "інформаційний тероризм" тощо).

Важливим напрямом у сфері інформаційної безпеки є пошук балансу між правами людини та потребою суспільства і держави в інформаційній безпеці, а також посилення юридичної відповідальності за використання в інформаційній сфері сил і засобів, які створюють загрози життю і здоров'ю людини. Крім того, актуальним залишається розробка сучасних моделей інформаційної безпеки [9].

До основних правових механізмів протидії загрозам інформаційній безпеці можна віднести кодифікацію інформаційного законодавства України та його гармонізацію з нормами і стандартами міжнародного інформаційного права, а також здійснення прикладних досліджень і розробок у сфері інформатизації та правової інформатики.

Кодифікація інформаційного законодавства та розвиток інформаційної сфери повинні бути засновані на наступних принципах:

— верховенство права;

— гарантованість права на інформацію, додержання інформаційних прав і свобод людини і громадянина;

— захищеність персональних даних, особистого та сімейного життя людини;

— забезпечення свободи інформаційної діяльності та вільного доступу до інформаційних ресурсів, крім винятків, визначених законами;

— захищеність національних інтересів і дотримання балансу інтересів людини, суспільства і держави в інформаційній сфері;

— формування правових засад для розвитку виробництва вітчизняних інформаційних технологій, ресурсів, продукції та послуг;

— гарантованість інформаційної безпеки та незворотність юридичної відповідальності за правопо-

рушення.

Для здійснення кодифікації інформаційного законодавства необхідна розробка та прийняття Інформаційного кодексу України, як основного закону в інформаційній сфері.

Важливе місце у правовому полі повинні займати систематизація, удосконалення і подальший розвиток законодавства України за окремими функціональними сегментами інформаційної сфери.

Основними напрямами прикладних досліджень і розробок у сфері правової інформатики можуть бути наступні:

— дослідження актуальних проблем правової інформатики та системної інформатизації нормотворчої, правозастосовної і правоосвітньої діяльності;

— розробка і впровадження інформаційно-правових підсистем електронного парламенту та електронного уряду;

— розробка електронних систем і баз даних у галузі держави і права;

— опрацювання технологічно-правових основ формування і розвитку електронно-мережевої економіки, електронного банкінгу тощо;

— розробка технологічно-правових засад захисту баз персональних даних, інформації з обмеженим доступом і технічного захисту інформації.

ВИСНОВКИ

Таким чином, реалізація зазначених досліджень і розробок, систематизація та удосконалення нормативно-правових актів за окремими функціональними сегментами інформаційної сфери сприятиме розвиткові інформаційного законодавства та більш ефективному забезпеченню інформаційної безпеки в умовах сучасної глобалізації та інтеграції України до світового інформаційного простору.

Література:

1. Закон України "Про інформацію" // Відомості Верховної Ради (ВВР). — 1992. — № 48. — Ст. 650.
2. Указ Президента України від 06.12.2001 р. № 1193/2001 "Про рішення Ради національної безпеки і оборони України" від 31 жовтня 2001 року з питання "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки".
3. Антимонов С. Для борьбы с компьютерным терроризмом требуются согласованные и скоординированные усилия разных государств и ведомств // "Безпека інформації в інформаційно-телекомунікаційних системах": Тези доп. учасників 6-ї Міжнар. наук.-практ. конф., 13—16 трав. 2003 р.
4. Гавловський В.Д., Цимбалюк В.С. Суспільні інформаційні відносини — об'єкт кримінально-правової охорони і захисту: кримінолого-когнітологічні аспекти // Боротьба з організованою злочинністю і корупцією (теорія і практика). — 2011. — № 4. — С. 168—167.
5. Гурковський В.І. Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання // Вісн. УАДУ. — 2002. — № 3. — С. 27—32.
6. Доктрина информационной безопасности Российской Федерации // Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. — М.: Академический Проект; Фонд "Мир", 2003. — С. 344.
7. Інформація буде захищена // Уряд, кур'єр. — 5 лип. — 2003. — № 122. — С. 11.
8. Ліпкон В.А. Теоретичні основи та елементи національної безпеки України: монографія. — К.: Текст, 2003. — С. 333—343.
9. Логінов О.М. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління // Науковий вісник Юридичної академії Міністерства внутрішніх справ: збірник наукових праць. — 2003. — № 3. — С. 199—204.

Стаття надійшла до редакції 20.02.2013 р.

ДО УВАГИ АВТОРІВ!

ВИМОГИ ДО СТРУКТУРИ ТА ОФОРМЛЕННЯ МАТЕРІАЛУ:

— відомості про автора (авторів): ім'я, по батькові, прізвище, вчене звання, вчений ступінь, посада і місце роботи, службова і домашня адреси (з поштовим індексом), контактний телефон;

— УДК;

— назва статті мовою оригіналу та англійською мовою;

— коротка анотація (2—4 речення) мовою оригіналу та англійською мовою;

— ключові слова;

— текст статті повинен мати такі необхідні елементи: вступ (формулюється наукова проблема, ступінь її вивченості, актуальність тієї частини проблеми, якій присвячена стаття), постановка задачі (формулюються мета і методи дослідження), результати (викладається система доведень запропонованої гіпотези, обгрунтовуються наукові результати), висновки (вказується наукова новизна, теоретична і практична значущість результатів дослідження, перспективи подальших розробок з цієї теми). Розділи повинні бути виділені;

— обов'язковий список використаних джерел у кінці статті;

— обсяг статті — 12—25 тис. знаків (як виняток, не більше 40 тис. знаків);

— шрифти найпоширенішого типу, текстовий шрифт та шрифт формул повинні бути різними;

— ілюстративний матеріал повинен бути поданий чітко і якісно у чорно-білому вигляді. Посилання на ілюстрації в тексті статті обов'язкові. До графіків та діаграм мають бути подані таблиці, на основі яких вони збудовані;

— разом із друкованою статтею треба подати її електронний варіант на CD носії або електронною поштою. Файл статті повинен бути збережений у форматі DOC для MS Word. Схеми, рисунки та фотографії слід записувати окремими графічними файлами форматів TIF, BMP, JPG, в імені яких зазначається номер ілюстрації у статті, наприклад pict 4.tif.

Редакція залишає за собою право на незначне редагування і скорочення, а також літературне виправлення статті (зі збереженням головних висновків та стилю автора). Надані матеріали не повертаються.

Адреса редакції: 04112, м. Київ, вул. Дорогожицька, 18, к. 29
для листування: 04112, м. Київ, а/с 61; economy_2008@ukr.net
Тел.: (044) 458-10-73, 223-26-28, 537-14-33