

Н. С. Грабар, кандидат наук з державного управління, науковий співробітник наукового відділу проблем державної безпеки навчально-науково-виробничого центру, Національний університет цивільного захисту України

Hrabar N.S., PhD in Public Administration, Researcher of State Security Research Department of Educational-scientific-production center, National University of Civil Protection of Ukraine, Kharkiv

ЗАРУБІЖНИЙ ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

FOREIGN EXERCISE OF LEGAL REGULATION OF SECURITY OF INFORMATION SECURITY

Наукова стаття присвячена дослідженню правового регулювання забезпечення інформаційної безпеки в контексті зарубіжного досвіду. У статті з урахуванням комплексного науково-методологічного аналізу висвітлені окремі особливості правового регулювання інформаційної безпеки у різних країнах світу. Зарубіжний досвід свідчить, що державні органи відіграють вирішальну роль в координації дій суб'єктів у сфері забезпечення інформаційної безпеки. Пріоритетним напрямком стає вдосконалення законодавства, що встановлює відповідальність за правопорушення, розробка та законодавче закріплення переліку правопорушень та видів відповідальності в сфері інформаційної безпеки.

Інформаційна безпека в силу глобального характеру мереж зв'язку може бути забезпечена лише при міжнародній взаємодії. У зв'язку з цим необхідно посилити взаємодію України із закордонними країнами, міжурядовими організаціями з питань правового забезпечення інформаційної безпеки.

Зроблено, висновок, що у практиці зарубіжних держав важливе місце займають питання забезпечення відкритості та доступу до публічної інформації, яка, однак, в більшості випадків розуміється широко – як будь-яка інформація, що знаходиться в розпорядженні державного сектора. Інформаційна безпека в силу глобального характеру мереж зв'язку може бути забезпечена лише при міжнародній взаємодії.

Ключові слова: інформаційна безпека, зарубіжний досвід, правове регулювання, забезпечення інформаційної безпеки, державне управління.

The scientific article is devoted to the study of legal regulation of information security in the context of foreign experience. In the article, taking into account the complex scientific-methodological analysis, some specific features of legal regulation of information security in different countries of the world are highlighted. Foreign experience shows that public authorities play a decisive role in coordinating the actors in the field of information security. The priority is to improve the legislation that establishes liability for offenses, to develop and legislatively establish a list of offenses and types of responsibility in the field of information security.

Information security due to the global nature of communication networks can only be provided with international interaction. In this regard, it is necessary to strengthen the interaction of Ukraine with foreign countries, intergovernmental organizations on issues of legal security of information security.

It is concluded that in the practice of foreign states the issue of ensuring openness and access to public information, which in the majority of cases is understood broadly – as any information available at the disposal of the public sector, occupy an important place. Information security due to the global nature of communication networks can only be provided with international interaction.

Keywords: information security, foreign experience, legal regulation, information security, public administration.

Постановка проблеми. Протягом останніх століть досягнення природничо-наукової культури породжували проблеми гуманітарної культури. Техніка, будучи підсилювачем здібностей людини, завжди кидала виклик праву, бо використовувалася не тільки на благо, але і на шкоду особі, суспільству і державі. Єдність і боротьба протилежностей двох культур особливо посилюється при переході людства від епохи підсилювачів фізичних здібностей людини в енергетичній сфері до епохи підсилювачів розумових здібностей в інформаційній сфері. Такими підсилювачами, як відомо, є засоби обчислювальної техніки і зв'язку, які суттєво змінюють просторово-тимчасові характеристики суспільних відносин і породжують нові, раніше невідомі види девіантних відносин. Панівною соціальною групою в суспільстві стають власники інформації та ноу-хау технологій, суспільство трансформується з постіндустріального до інформаційного. Змінюється геополітичне інформаційне протиборство держав, яке все частіше набуває форми планомірних інформаційних операцій під прикриттям принципу свободи інформації.

Нинішній етап розвитку інформаційних технологій характеризується можливістю масованого інформаційного впливу на індивідуальну і суспільну свідомість аж до проведення великомасштабних інформаційних воєн, в результаті чого неминучим противагою принципу свободи інформації стає принцип інформаційної безпеки. Цей принцип обумовлений глобальною інформаційною революцією, стрімким розвитком і повсюдним впровадженням новітніх інформаційних технологій і глобальних засобів телекомунікацій. Проникаючи в усі сфери життєдіяльності держав, інформаційна революція розширює можливості розвитку міжнародного співробітництва, формує планетарний інформаційний простір, в якому інформація набуває властивостей найціннішого елемента національного надбання, його стратегічного ресурсу.

Разом з тим, стає очевидним, що поряд з позитивними моментами такого процесу створюється і реальна загроза використання досягнень в інформаційній сфері, в цілях, не сумісних із завданнями підтримки світової стабільності і

безпеки, дотриманням принципів суверенної рівності держав, мирного врегулювання суперечок і конфліктів, незастосування сили, невтручання у внутрішні справи, поваги прав і свобод людини. Наявна в Україні система правових норм не повною мірою відображає потреби забезпечення інформаційної безпеки. Системна робота в сфері правового забезпечення інформаційної безпеки потребує наукового обґрунтування подальшої розробки таких нормативних актів, в яких би в повній мірі були враховані міжнародні принципи і норми, спрямовані на зміцнення міжнародної інформаційної безпеки та разом з тим максимально враховувалися національні інтереси.

Аналіз останніх досліджень і публікацій. Проведений доктринальний аналіз проблем інформаційної безпеки засвідчив, що, незважаючи на величезний інтерес до даної проблематики, її вивчення має переважно техніко-прикладний характер і орієнтоване на рішення конкретних науково-технічних завдань.

Дослідженню теоретико-практичних аспектів інформаційної безпеки, зверненого до ролі інформаційних процесів, присвячені роботи вітчизняних вчених О. Бодрука, А. Качинського, В. Крисаченка, С. Пирожкова, Т. Стародуб, О. Шевченка, водночас проблеми правового регулювання забезпечення інформаційної безпеки в контексті зарубіжного досвіду вченими не розглядались, що й зумовило науковий інтерес авторки.

Внаслідок чого **метою** даної статті є узагальнення міжнародного досвіду правового регулювання інформаційної безпеки та обґрунтування концептуальних положень системи правового регулювання в сфері забезпечення інформаційної безпеки України.

Виклад основного матеріалу. Серед численної кількості міжнародних законодавчих актів, чітко простежується теза про те, що інформаційна та мережева безпека розуміється – це здатність мережі або системи протистояти з певним рівнем надійності аварій або зловмисних дій, що можуть порушити доступність, цілісність і конфіденційність інформації, що зберігається або передається інформації, а також послуг, що надаються за допомогою мережі

або інформаційної системи. Дотримання безпеки визначається як доступність, ідентифікація, цілісність, конфіденційність інформації. Особлива увага при цьому приділяється законодавчій базі, яка зачіпає питання перехоплення і дешифрування інформації.

Так, в Законі США «Про управління інформаційною безпекою» від 2002 року інформаційна безпека визначається як: захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, поширення, модифікації або знищення; забезпечення цілісності інформації від неправомірної зміни або знищення, включаючи гарантії її справжності; забезпечення конфіденційності, що означає підтримку встановлених обмежень доступу і поширення інформації, включаючи закритість даних про приватного життя і про власність; доступність, що означає швидкий і надійний доступ до інформації.

Для багатьох зарубіжних держав в основному характерний підхід до проблеми інформаційної безпеки з урахуванням таких понять, як «автентичність», «доступність», «цілісність», «конфіденційність».

Закон США «Про захист інформації» від 1998 року призводить аналогічний закон 1984 року в відповідність до Директиви 95/46 ЄС Європейського парламенту та Ради Європейського Союзу «Про захист прав приватних осіб стосовно обробки персональних даних» і поширює його на облікові записи, які ведуться державними установами та приватними компаніями, а також встановлює ряд обмежень на використання персональних даних та на доступ до облікових записів [1, с. 150-152].

Питання недоторканності приватного життя регулюються в ряді інших законодавчих актів США, наприклад в законах, що регламентують ведення медичних записів і зберігання інформації про споживчі кредити, а також в Законах «Про реабілітацію правопорушників» 1974 року, «Про телекомунікації» 1984 року тощо.

Одним з найстаріших законів прийнято вважати Закон «Про свободу друку» 1776 року прийнятий в Швеції, який передбачає право доступу

громадян до інформації про діяльність органів державної влади, і в даний час сфера його дії поширюється на всі види документів, включаючи електронні.

У ряді країн Європи, таких як Нідерланди, Іспанія, Португалія, Австрія, Угорщина, Естонія, Бельгія та Румунія, право громадян на доступ до офіційної інформації закріплено конституційно. У Франції, Греції та Італії ці права закріплені в законах. Удосконалення законодавства в даній сфері триває в Великобританії, Німеччині, Естонії, Молдові, Польщі та ряді інших держав.

Так, у Швеції і Фінляндії законодавчо встановлено обмеження прав на доступ до урядової інформації. Сьогодні важливо відзначити і іншу тенденцію в зарубіжних країнах, як втім і в Україні, – це розробка і реалізація концепцій електронного уряду, що ґрунтується на застосуванні інформаційних технологій при створенні державних інформаційних ресурсів та доступу до інформації про діяльність державних органів влади, відкритих даних (США, Сінгапур, Австралія, Нова Зеландія та ін.) [2, с. 130].

В Австрії, наприклад, також законодавчо закріплено право громадян на доступ до нормативно-правової бази, при цьому інформація знаходиться в розпорядженні державного сектора, а не комерційних структур (стягується плата за копіювання та розповсюдження).

Таким чином, аналіз зарубіжного досвіду правового регулювання питань доступу до інформації свідчить не тільки про загальні тенденції, а й про різні підходи до правового регулювання питань забезпечення інформаційної безпеки.

Значний масив законодавчих та інших нормативних правових актів у галузі забезпечення інформаційної безпеки в багатьох зарубіжних державах стосується електронної торгівлі та використання електронних підписів: Закон Канади «Про електронні угоди» 1999 року, Федеральний закон США «Про електронні підписи в міжнародній і внутрішній торгівлі» 2000 року, Закон Ірландії «Про електронну торгівлю» 2000 року, Закон Іспанії «Про послуги інформаційного суспільства та електронної торгівлі» 2002 року, Закон Південної Кореї «Про електронну торгівлю» 2001 року, Закон Таїланду «Про електронні угоди і електронного підпису» 2002 року тощо [3, 4, 5, с. 131].

Аналіз стану правового регулювання в даній сфері в розглянутих зарубіжних державах показує, що нормативні правові акти, що регулюють захист інформації, інформаційної техніки і технологій, спрямовані на створення і захист інформаційних мереж, що встановлюють єдині умови використання ліній зв'язку та комунікаційних послуг, діють уже в більшості держав .

На особливу увагу в області правового забезпечення інформаційної безпеки заслуговують питання захисту персональних даних, регламентовані в багатьох державах. Наприклад, в Іспанії ще в 1999 р був прийнятий Органічний закон «Про захист персональних даних», згідно з яким загальнодоступними джерелами є: списки висунутих на посаду кандидатів, телефонні довідники (відповідно до законодавства) і списки осіб за професіями, що містять інформацію про імена, звання, професії, рід діяльності, а також офіційні видання, бюлетені і ЗМІ [6, с. 201].

Разом з тим необхідно відзначити, що в Україні завершена майже семирічна процедура, пов'язана з ратифікацією одного з найактуальніших міжнародних правових актів у сфері захисту прав людини в процесі використання сучасних інформаційно-комунікаційних технологій – Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних 1981 р . Таким чином, зроблено значний крок на шляху до повноформатної участі України в зусиллях держав – членів Ради Європи зі зміцнення безпеки людини в кіберпросторі та загальноєвропейському правовому просторі. Однак процес модернізації зазначеної Конвенції, в якому Україна задіяна в якості повноправного учасника, все ще триває, чим і викликане динамічний розвиток, видання підзаконних актів та інших нормативно-правових актів.

Однією з найактуальніших в даний час в усьому світі є проблема правового регулювання в мережі Інтернет. Глобальна інформаційно-телекомунікаційна мережа Інтернет поряд з об'єктивними благами, які вона дає людству, ввібрала в себе багато проблем суспільства, що проявилися у виникненні нових форм (видів) протиправної діяльності і виникнення нових загроз, несумісних із завданнями підтримки світової стабільності і безпеки.

Завдання щодо забезпечення протидії тероризму і екстремізму відображені в державній політиці багатьох зарубіжних держав, і аналіз правового регулювання в цій сфері дозволяє зробити висновок про тенденцію до посилення відповідальності за кібертероризм і поширення протиправної інформації [7, с.18].

Особливий інтерес і критику в світі викликає політика Китаю, де починаючи з 2000 року створені спеціальні підрозділи кіберполіції для підтримки порядку в мережі Інтернет і особлива увага приділяється вдосконаленню засобів контролю за інтернет-простором, створені «кібервійська», в той же час важливим питанням є застосування так званої «мудрої сили», тобто поліпшення іміджу держави.

Ключову роль продовжує відігравати американський Закон «Про інформаційну безпеку» 1987 року, головна мета якого реалізація мінімально достатніх дій щодо забезпечення безпеки інформації в федеральних комп'ютерних системах без обмежень всього спектру можливих дій. Згідно з цим Законом всі оператори федеральних інформаційних систем, що містять конфіденційну інформацію, повинні сформулювати плани забезпечення інформаційної безпеки, а всі урядові відомства повинні сформулювати план забезпечення інформаційної безпеки, спрямований на те, щоб компенсувати ризики і запобігти можливих збитків від втрати, неправильного використання, несанкціонованого доступу або модифікації інформації в федеральних системах [8, с.85].

Висновки. Таким чином, зарубіжний досвід свідчить, що державні органи відіграють вирішальну роль в координації дій суб'єктів у сфері забезпечення інформаційної безпеки. Пріоритетним напрямком стає вдосконалення законодавства, що встановлює відповідальність за правопорушення, розробка та законодавче закріплення переліку правопорушень та видів відповідальності в сфері інформаційної безпеки.

Інформаційна безпека в силу глобального характеру мереж зв'язку може бути забезпечена лише при міжнародній взаємодії. У зв'язку з цим необхідно

посилити взаємодію України із закордонними країнами, міжурядовими організаціями з питань правового забезпечення інформаційної безпеки. Аналіз зарубіжного законодавства, що регулює інформаційну сферу, дозволяє стверджувати, що в сфері правового регулювання права на інформацію, доступу до інформації, ЗМІ, а також обмеження свободи інформації відбулися істотні зміни. Проведений аналіз міжнародних і зарубіжних правових актів в інформаційній сфері свідчить про те, що є значний і різноманітний досвід правового регулювання як на міжнародному, так і на національному рівнях.

У практиці зарубіжних держав важливе місце займають питання забезпечення відкритості та доступу до публічної інформації, яка, однак, в більшості випадків розуміється широко – як будь-яка інформація, що знаходиться в розпорядженні державного сектора. Інформаційна безпека в силу глобального характеру мереж зв'язку може бути забезпечена лише при міжнародній взаємодії.

Список використаних джерел:

1. Скалацький В. М. Інформаційне суспільство: сучасні теорії та моделі (соціальнофілософський аналіз): дис.: 09.00.03 / В. М. Скалацький. — Київ : Київ. нац. ун-т ім. Тараса Шевченка, 2006. — 181 с.
2. Почепцов Г. Г. Інформаційна політика: навч. посіб. / Г. Г. Почепцов, С. А. Чукут. — Київ : Знання, 2006. — С. 130–211.
3. Information Superhighway: An Overview of Technology Challenges [Доповідь Конгресу США] / USA Congress. — Washington, 1995.
4. Building the Information Society: Moving Canada into the 21st Century [Нормативний документ Міністерства Постачання та Послуг Канади] / Ministry of Supply and Services. — Ottawa, 1996.
5. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України: дис. ... д-ра політ. наук: спец. 23.00.02. / О. В. Соснін; Одес. нац. юрид. акад. — Одеса, 2005. — 264 с.
6. Туманова Л. В. Обеспечение и защита права на информацию / Л. В. Туманова, А. А. Снытников. — Москва : Городец-издат, 2001. — 345 с.

7. Конах В. К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США) автореф. дис ... канд. політ. наук: 21.01.01 / Вікторія Констянтинівна Конах. Нац. ін-т стратег. дослідж. – К., 2005. – 20 с.

8. Почепцов Г. Г. Інформаційна політика та інформаційні війни: навч.-метод. посіб. / Г. Г. Почепцов. – К.: Вид-во НАДУ, 2012. – 120 с.

References:

1. Skalatskyy V. M. Information society: modern theories and models (socio-philosophical analysis): diss.: 09.00.03 / V.M. Scalatsky. - Kyiv: Kiev. Nats Untitled Taras Shevchenko, 2006. - 181 pp.

2. Pocheptsov G. G. Information Policy: Teach. manual / G. G. Pocheptsov, S. A. Chukut. - Kyiv: Knowledge, 2006. - P. 130-211.

3. Information Superhighway: An Overview of Technology Challenges / U. S. Congress. - Washington, 1995.

4. Building the Information Society: Moving Canada into the 21st Century [Ministry of Supply and Services Legislation]. - Ottawa, 1996.

5. Sosnin O. V. State policy in the field of management of information resources of Ukraine: diss. ... doctor is flying. Sciences: special 23.00.02. / O. V. Sosnin; Odessa Nats Lawyer Acad. - Odessa, 2005. - 264 p.

6. Tumanova L.V. Provision and protection of the right to information / L.V. Tumanova, A. A. Snytnikov. - Moscow: Gorodets-Izdat, 2001. - 345 p.

7. Konah V. K. Providing information security of the state as a component of the national security system (US example). Author's abstract. Dis ... Cand. flight. Sciences: 21.01.01 / Viktoriya Konstantinovna Konakh. National other strategist research - K., 2005. - 20 p.

8. Pocheptsov G. G. Informational politics and information wars: teaching method. manual / G. G. Pocheptsov. - K.: View at NAPA, 2012. - 120 p.