Maruhovsky O. Conflict of civilizations in the modern globalized world: geopolitical and religious dimensions

This article explores the nature of main (geopolitical and religious) aspects of the conflict of civilizations; reveals the essence and influence of globalization and Westernization on the geopolitical situation in the world.

Keywords: *globalization, Westernization, civilization, civilizations conflict, Islamic civilization, western civilization.*

УДК 316.32:325.455(73)

Морозова Вероніка Олексіївна,
студентка спеціальності «Політологія» НПУ імені М.П. Драгоманова

ДЕРЖАВНА ПОЛІТИКА ТА СТРАТЕГІЇ США У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛЬНИХ ВИКЛИКІВ

В статті розглядаються сутність політики США у сфері інформаційної безпеки; основні пріоритети державної політики у сфері інформаційної безпеки, що полягають у створення чіткої стратегії як засобу посилення безпеки та надійності інформаційних систем держави.

Ключові слова: *інформація; інформаційна безпека; національна безпека; інформаційні загрози; інформаційні технології; інформаційні стратегії.*

Вперше поняття «інформаційна безпека» було вжито в США в концепції національної безпеки у 1947 році як складова національної безпеки держави. Також поняття «національна безпека» вперше з'явилося у політичному лексиконі в США у 1904 році у посланні президента Т. Рузвельта до Конгресу, де він обґрунтував приєднання зони Панамського каналу інтересами «національної безпеки».

Інформаційна безпека (information security) – збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність [5, с. 3].

Інформаційна безпека держави – стан захищеності життєвоважливих інтересів людини, суспільства і держави, при якому запобігається нанесення 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 [1].

Розвиток і використання інформаційно-комунікаційних технологій (ІКТ) є глобальною тенденцією світового розвитку останніх десятиліть. Застосуванню ІКТ належить важливе значення для підвищення конкурентоздатності економіки, розширення можливостей її інтеграції у світову систему господарства, підвищення ефективності державного керування та місцевого самоврядування. Світовий обсяг виробництва інформаційної техніки та інформаційних технологій на початку XXI століття перевищив трильйон доларів.

Та зростає й потенційна уразливість суспільних процесів від інформаційного впливу. Сьогодні інформація є чинником, здатним призвести до масштабних аварій, військових конфліктів, дезорганізації державного управління, фінансових органів і наукових центрів. Інформаційні технології використовуються як політичний інструмент.

Інформаційні війни, інформаційний тероризм – форми та прийоми для вирішення широкого кола завдань локального та стратегічного характеру. У зв'язку з цим питання інформаційної безпеки громадянина, суспільства, держави набуває все більшої актуальності. Захист інформації, яка передається, зберігається та обробляється за допомогою

телекомунікаційних систем різних типів в умовах широкого застосування комп'ютерної техніки та інформаційних технологій виходить сьогодні на перший план.

Невизначеність на глобальному рівні та відсутність узгоджених стандартів змушує керівництво окремих держав формувати політику інформаційної безпеки на національному рівні. США розробила власні стратегії [10].

Говард Шмідт зазначав, що основним пріоритетом державної політики має бути створення чіткої стратегії як засобу посилення безпеки та надійності інформаційних систем держави.

США є лідером у області інформаційно-телекомунікаційних технологій. На початку 90-х років у структурі бізнесу США відбувся поворот на користь компаній, що спеціалізуються в інформаційній сфері. Новітні технології, Інтернет змінюють структуру економіки США.

У США під патронажем Національного наукового фонду в рамках державного проекту ARPANET було створено мережу Інтернет. З тих пір американський уряд продовжує надавати великі кошти для проведення досліджень та розробок в області Інтернету. Одночасно закон про скасування оподатковування Інтернету наклав мораторій на стягнення податків з угод в області електронної комерції.

Політика державної підтримки та розвитку ІКТ у США починається з Телекомунікаційного акту 1934 року. У 1978 році засновано спеціальну організацію з розвитку ІКТ-сектора (National Telecommunications and Information Administration). Проте основа сучасної державної політики США у області інформаційних технологій була закладена у 1996 році із прийняттям Телекомунікаційного акту 1996 року, який став значною зміною законодавства США у області інформаційних технологій із часів Телекомунікаційного Акту 1934 року. Ідея даного законодавчого документу полягала в тому, що виробники товарів та послуг ІКТ-сектора не повинні бути лімітовані штучними та застарілими обмеженнями, проте одночасно мають конкурувати один з одним на стабільному ринку, що включає велику кількість акторів.

Перший закон про захист інформації був прийнятий в 1906 році. Проте усвідомлення США стратегічної ролі інформаційного впливу та інформаційної безпеки почалось у 80-ті роки з приходом до влади адміністрації Р.Рейгана. При ньому склалась чітка організаційна структура державного управління у сфері інформаційної безпеки з відповідним розподілом компетенцій та повноважень державних органів усіх рівнів.

Головним державним органом у процесі координації роботи інформаційних структур США під час розробки та реалізації загальнодержавних рішень у сфері захисту інформації стала Рада національної безпеки (РНБ), на яку було покладено розробку стратегічної концепції інформаційної безпеки країни, правових та організаційних механізмів регулювання міжвідомчої взаємодії. Серед міністерств (відомств) США, які відповідають за формування та реалізацію державної політики у сфері інформаційної безпеки в галузі телекомунікацій ключовими є Агентство національної безпеки (АНБ) – орган, у якому зосереджені функції щодо реалізації державної політики у сфері криптографічного та технічного захисту інформації, захисту державних інформаційних ресурсів і державного контролю за станом безпеки інформації в інформаційно-телекомунікаційних системах та Національний інститут стандартів і технологій (НІСТ), відповідальний за випуск стандартів і керівних документів, спрямованих на захист від знищення та несанкціонованого доступу до інформації.

У січні 1983 року Р.Рейган підписав директиву «Керівництво державною дипломатією, пов'язане з цілями національної безпеки», яка до дипломатичної діяльності включила заходи уряду США, спрямовані на підтримку політики національної безпеки шляхом організації та проведення широкого кола інформаційних заходів.

Певну роль у формуванні державної політики США у сфері інформаційної безпеки відіграли прийняті у 80-ті роки Конгресом закони «Про скорочення паперової документації» (Paper Reduchion Act) та «Про свободу інформації» (Freedom Information Act) [6, с. 88], які

підняли управління інформаційними ресурсами до рангу урядової політики. Ключовим в реалізації забезпечення безпеки інформації у федеральних інформаційно-комунікаційних системах, став «Закон про інформаційну безпеку» (Computer Security Act) [7]. Відповідно до Закону, всі оператори федеральних інформаційно-комунікаційних систем, що містять конфіденційну інформацію, повинні сформувати плани забезпечення інформаційної безпеки. На початку 90-х років міністерствами та відомствами США, які відповідають за національну безпеку, створюється Об'єднана комісія з питань безпеки. Ця комісія розробила нові підходи до формування політики інформаційної безпеки [2, с. 45-68].

Новим етапом у вирішенні проблем захисту інформаційної інфраструктури у США стало формування адміністрацією Б.Клінтона у 1996 році Президентської комісії з захисту критичної інфраструктури. Звітна доповідь цієї комісії, опублікована в жовтні 1997 року, виявила уразливість національної безпеки США в інформаційній сфері та закликала вжити загальнодержавних заходів. Підсумки роботи комісії було покладено в основу урядової політики у сфері забезпечення інформаційної безпеки інформаційно-комунікаційних систем.

Закон «Про вдосконалювання інформаційної безпеки» (Computer Security Enhancement Act) прийнятий у 1997 році, який був спрямований на посилення ролі НІСТ та залучення приватного сектору для забезпечення захисту інформації в телекомунікаційних системах.

В директиві президента США Б.Клінтона № 63 від 22 травня 1998 року зазначається, що Б.Клінтон має намір забезпечити прийняття США необхідних заходів для швидшого усунення усіх недоліків, які роблять найголовніші об'єкти інфраструктури, комп'ютерні системи уразливими до фізичного та комп'ютерного нападів.

Для виконання завдань, визначених у директиві було розроблено національний План захисту інформаційних систем США, підписаний президентом. План повинен був стати початком довгострокової загальнонаціональної програми у сфері інформаційної безпеки. План містив 10 самостійних програм, об'єднаних загальною метою [11]. Назвемо основні з них:

1. Програма по формуванню Федеральної Служби комп'ютерної підготовки та навчання. Ця програма спрямована на поліпшення ефективності залучення й утримання високо кваліфікованої робочої сили в урядових закладах, включаючи збільшення чисельності кваліфікованих фахівців в області інформаційної безпеки.
2. Програма по формуванню Федерального Центру підвищення кваліфікації в області інформаційно-телекомунікаційних технологій (CIET). CIET повинна забезпечити перепідготовку працюючих адміністраторів федеральних інформаційно-телекомунікаційних систем і фахівців з інформаційної безпеки.
3. Програма навчання учнів середньої школи та викладачів, а також широкої публіки з питань інформаційної безпеки.
4. Програма навчання проблем інформаційної безпеки серед федеральних службовців.
5. Програма створення постійно діючої Федеральної Групи експертного контролю.
6. Програма створення Федеральної мережі виявлення вторгнення (FIDNET) є мережею виявлення вторгнень в інформаційно-телекомунікаційні системи цивільних урядових агентств.
7. Програма Формування інфраструктури керування відкритими ключами засобів криптографічного захисту інформації.

Адміністрацією Дж. Буша було прийнято два стратегічних документи, спрямованих на захист інформаційних ресурсів держави: «Національна стратегію фізичного захисту критичної інфраструктури» (The National Strategy for Physical Protection of Critical Infrastructures and Key Assets) та «Національну стратегія кібернетичної безпеки» (The The National Strategy to Secure Cyberspace) [4].

Нові стратегії вперше офіційно визнають уразливість та залежність інфраструктури США від інформаційних систем і мереж. Вони спрямовують уряд, промисловість, бізнес та суспільство на створення «Єдиної національної системи реагування на кібернетичні напади»

(National Cyberspace Secure Response System), що являє собою сукупність територіальних, відомчих і приватних центрів аналізу та розподілу інформації у різних секторах народного господарства та економіки країни. Національною стратегією боротьби з тероризмом (The National Strategy for Combating Terrorism), прийнятою адміністрацією Дж. Буша, поняття «кібернетичного тероризму» визначено як «навмисне руйнування, переривання чи перекручування даних у цифровій формі чи потоків інформації, які мають широкомасштабні наслідки в політичному, релігійному чи ідеологічному плані» [12].

Стратегія кібернетичної безпеки США побудована за п'ятьма пріоритетними напрямами діяльності: національна система реагування на загрози для безпеки кіберпростору; національні заходи зменшення загрози та уразливості кіберпростору; освіта та навчання з питань захисту кіберпростору; заходи щодо захисту кіберпростору органів влади; співробітництво з питань національної безпеки та безпеки міжнародного кіберпростору [4].

Глобальна структура системи Інтернет досить ускладнює здійснення заходів окремою державою щодо захисту її національного сектору. Кіберпростір будь-якої держави пов'язаний з усім світом, тому встановити джерело кібератаки без належного міжнародного співробітництва іноді неможливо. Американці намагаються вирішити цю проблем шляхом системи заходів, спрямованих на досягнення високої ефективності контррозвідувальної діяльності в кіберпросторі: підвищення спроможності встановлення джерел кібератак та реалізації заходів у відповідь; удосконалення координації діяльності органів національної безпеки США у питаннях реагування на кібератаки; співробітництво з приватним сектором і робота по лінії міжнародних організацій з метою розвитку діалогу і партнерства із зарубіжними урядами та приватним сектором, з акцентом на захисті інформаційних інфраструктур та популяризації глобальної «культури безпеки».

У вересні 2001 року Конгресом США був прийнятий «Закон про посилення повноважень спецслужб», що визначив несанкціоноване проникнення в державні інформаційно-комунікаційні мережі однією з форм тероризму. Даний Закон спростив процедуру моніторингу Інтернету з боку ФБР. 26 жовтня 2001 року Конгрес США ухвалив «Закон про патріотизм», який надав уряду, поліції та федеральним агентствам широкі повноваження з нагляду за громадянами. Наступний «Закон про боротьбу з тероризмом» (Combating Terrorism Act) [8] розширив повноваження спецслужб, пов'язаних з інформаційним моніторингом та стеженням в Інтернеті.

Відповідно до ухваленого Конгресом США у 2002 році «Закону про внутрішню безпеку» (Homelend Security Act) урядові структури, які займалися комп'ютерною безпекою, перейшли під контроль новоствореного Міністерства внутрішньої безпеки (Department of the Homelend Security). В інтересах захисту інформаційних ресурсів у ст. 225 цього закону окреслено додаткові заходи, які спрямовані на посилення відповідальності за злочини у сфері високих технологій. Вони в свою чергу оформлені у вигляді «Закону про посилення кібернетичної безпеки» (Cyber Security Enhancement Act).

США залишаються одним з основних гравців, що визначають перспективи розвитку кіберпростору й потенційні напрями в його регулюванні (або формуванні політики щодо даного питання). Головна зовнішньополітична ініціатива США щодо перспектив розвитку кіберпростору була оприлюднена 16 травня 2011 р. під назвою Міжнародна стратегія для кіберпростору (International Strategy for Cyberspace) [9]. Так, «базовими принципами», що мають бути забезпечені при формуванні політики щодо кіберпростору, Стратегія визначає:

1. «Фундаментальні свободи» (можливість шукати, отримувати й передавати інформацію та ідеї через будь-які засоби зв’язку та незважаючи на кордони).
2. «Прайвесі» (люди мають бути обізнані з загрозами їхній персональній інформації та про можливість здійснення проти них кіберзлочинів).

3. «Вільні потоки інформації» (рух інформації не має обмежуватися фільтрами, міжмережевими екранами, оскільки вони створюють видимість безпеки, кіберпростір має бути місцем інновацій та співпраці держави й бізнесу задля більшої безпеки [3, с. 4-5].

Отже, аналіз державної політики США у сфері інформаційної безпеки в галузі інформаційно-телекомунікаційних систем дозволяє зробити наступні висновки: 1) інформаційна безпека в США розглядається як невід'ємна складова національної безпеки держави; 2) сучасна інформаційна політика США забезпечує формування і розвиток цілісної системи державного управління у сфері інформаційної безпеки; 3) в країні створена ефективна організаційна структура і сформована необхідна законодавча база, яка будується на підставі загальнодержавної стратегії забезпечення інформаційної безпеки; 4) захист національного інформаційного простору набуло пріоритетного значення в інформаційній політиці США.

Література:

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007—2015 роки» [Електронний ресурс] від 09.01.2007 № 537-V // Режим доступу: http://zakon4.rada.gov.ua/laws/show/537-16.

2. Гуменюк Б. І. Сучасна дипломатична служба / Б. І. Гуменюк, О. В. Щерба. — К.: Либідь, 2001. — 255 с.

3. Дубов Д. В. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців : аналіт. доп. / Д. В. Дубов, М. А. Ожеван. – К.: НІСД, 2012. – 32 с.

4. Гнатцов О. Г. Інформаційні ресурси в системі забезпечення державної безпеки. Інформаційні відносини та технології / О. Г. Гнатцов. - 2004. — №2.

5. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. — К.: Національний банк України, 2010. – 49 с.

6. Устинов В. Н. Информационное превосходство США / В. Н. Устинов. — М., 1997.

7. Computer Security Act of 1987. Public Law 100-235 (H.R. 145), January 8, 1988.

8. Combating Terrorism Act of 2001, H.R. 3566.

9. International Strategy for Cyberspace [Електронний ресурс] // Режим доступу: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

10. Lewis James A., Timlin K. Cybersecurity and Cyberwarfare, Preliminary Assessment of National Doctrine and Organization, Center for Strategic and International Studies – 2011 [Електронний ресурс] / James A. Lewis, Katrina Timlin // Режим доступу: http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.

11. National Plan for Information Systems Protection [Електронний ресурс]. – Режим доступу:http//google.com.ua/search?q=cache:ZZOpQQXLr8MJ:www.treachery.net/~jdyson/texts/cybersecplan.htm+NSIRC&hi=uk.

12. The National Strategy for Combating Terrorism / February 2003. [Електронний ресурс]. – Режим доступу: http://2001-2009.state.gov/s/ct/rls/wh/71803.htm.

Морозова В. А. Государственная политика и стратегии США в сфере информационной безопасности в условиях глобальных вызовов

В статье рассматриваются сущность политики США в сфере информационной безопасности; основные приоритеты государственной политики в сфере информационной безопасности, которые заключаются в создании стратегии как средства повышения безопасности и надежности информационных систем государства.

Ключевые слова: *информация; информационная безопасность; национальная безопасность, информационные угрозы, информационные технологии, информационные стратегии.*

Morozova V. State policies and strategies in the U.S. information security in the global challenges

This article examines the nature of U.S. policy in the field of information security. The main priorities of the state policy in the field of information security is to create a clear strategy as a means of strengthening the safety and security of the information systems of the state.

Keywords: *information; information security; national security; information threats; information technology; information strategy.*

УДК 32-027.21:005.44.

Морозова Ольга Олексіївна,
кандидат політичних наук, доцент кафедри методики викладання суспільно-політичних дисциплін НПУ імені М.П. Драгоманова

ГЛОБАЛІЗАЦІЯ У СФЕРІ ПОЛІТИКИ

В статті розглядаються сутність поняття «глобалізація», глобалізація у сфері політики. Глобалізацію можна уявити в трьох вимірах: 1) як об'єктивну тенденцію світового економічного, соціального, політичного й культурного розвитку; 2) як мету, висунуту політичним керівництвом держав світу; 3) як методологію аналізу розвитку країн і міжнародних відносин.

Ключові слова: *глобалізація, держава, політика.*

Термін «глобалізація» міцно увійшов у науковий і політичний обіг, однак дослідники розуміють його по-різному. Найчастіше глобалізацію пов'язують з якісно новим рівнем інтегрованості, цілісності й взаємозалежності світу, хоча це лише частина більш складної й суперечливої картини.

Багато авторів, що присвятили праці проблемі глобалізації, вказують на неточність самого терміна. Справді, якщо й можна говорити про прагнення сучасного світу до більшої інтегрованості, то назвати цю тенденцію загальною і єдиною ніяк не можна. Деякі вчені вкрай критично ставляться до глобалізації, зазначаючи, що «чутки про глобалізацію сильно перебільшені». Крім того, викликає заперечення погляд на глобалізацію як на безальтернативний процес або принаймні провідну тенденцію. Дослідники вказують на паралельні глобалізації процеси: економічну й соціальну демодернізацію, культурну фрагментацію й сегментацію [4].

Фундаментом експансії світового суспільства щодо міжнародної спільноти стали як матеріальні, так і віртуальні новації, що узагальнюються у політологічному дискурсі розпливчастим і неточним словом «глобалізація». У літературі 1990-х років цей термін, на думку російського дослідника А. Батурова, у різних сполученнях використовувався на позначення щонайменше восьми основних тенденцій і явищ:

1) об'єктивне зростання проникності міждержавних кордонів (феномен «подолання кордонів» і «економічного громадянства»);

2) різке зростання обсягів та інтенсивності трансдержавних, транснаціональних перетікань капіталів, інформації, послуг і людських ресурсів;

3) масоване поширення західних стандартів споживання, побуту, само- і світосприймання на всі частини планети;

4) посилення ролі поза-, над-, транс- і просто недержавних регуляторів світової економіки й міжнародних відносин;

5) форсований експорт і вживлення в політичну тканину різних країн світу тих чи інших варіацій моделі демократичного державного устрою;

6) формування віртуального простору електронно-комунікаційного спілкування, що різко збільшує можливості для соціалізації особистості, тобто для безпосереднього