

Олійник Олег Вікторович –
головний консультант Інституту за-
конодавства Верховної Ради Украї-
ни, кандидат юридичних наук, стар-
ший науковий співробітник

Інформаційна безпека США

*У статті проаналізовано стан та сучасні тенденції забезпе-
чення інформаційної безпеки США.*

Ключові слова: інформаційна безпека, методи інформаційної безпеки, інформаційна інфраструктура, національна безпека.

Необхідність наукового аналізу форм і методів інформаційної безпеки, захисту населення від негативних впливів, як у воєнний час, так і в мирний, що використовується США, дозволить критично оцінити американський досвід у побудові інформаційної стратегії, в цілому розглянути її систему, роль і повноваження різних відомств з урахуванням специфіки їх діяльності. Вивчення теорії та практики інформаційних операцій, інформаційного протиробства, інформаційних війн, що проводяться США, необхідно для аналізу можливих загроз Україні.

Існує необхідність уточнення та розробки практичних рекомендацій щодо забезпечення інформаційної безпеки з метою захисту від інформаційних впливів на органи державної влади та управління України в інтересах підвищення ефективності інформаційної політики, забезпечення інформаційної безпеки особи, суспільства та держави [1, с. 5].

Ураховуючи те, що США мають значний фінансовий, технологічний, науково-технічний та воєнний потенціал, а також приділяють велику увагу посиленню національної безпеки, захисту громадянських прав та інтересів бізнесу, досвід цієї держави у сфері управління інформаційною безпекою є найбільш важливим для вивчення. Значимість управління інформаційною безпекою в США на державному рівні визначається також тим, що в цій державі сконцентровані найбільші фінансові компанії, дослідницькі центри та корпорації, які суттєво впливають на розвиток технологій, фінансову стабільність і економічний розвиток усього світового співтовариства.

Активізація процесу концептуального забезпечення національної безпеки розпочалась з прийняття Закону “Про національну безпеку” 1947 року, який заклав основу інституційного механізму її забезпе-

чення. Батьком теорії “політичного реалізму” для США є Г. Моргент-тау, який обґрунтував поняття “національний інтерес” як рушійну силу в міжнародних відносинах. Він також сформулював концепцію “світо-порядку”, в основі якого теорія балансу сил і положення про те, що політика держав визначається боротьбою за владу та вплив.

Окремі аспекти теорії національної безпеки розроблювались Т. Шелінгом і Г. Каном (теорія міжнародних конфліктів); Р. Лиска і Г. Снайдером (теорія блоків та коаліцій); К. Норром (теорія потенціалу держави); Зб. Бжезинським (геостратегічні моделі) Е. Люттвакум, М. Портером (міжнародна економічна конкуренція) та ін.

Поширення отримали прикладні роботи в сфері національної безпеки, спрямовані на обґрунтування тих чи інших аспектів політики США, а також концептуальні розробки національної стратегії. Організаційно їх робота виконувалась на базі дослідницьких центрів, що працюють на замовлення адміністрації США, комітетів конгресу, політичних партій.

На сьогодні у США практично оформилась, як один із розділів політології, теорія національної безпеки, яка включає наступні напрямки: концептуальні основи стратегічного бачення; прогнозування міжнародних відносин; національні доктрини і стратегії (концепції) національної безпеки; дипломатична стратегія; економічна стратегія; геостратегічне планування; військова стратегія та прогнозування, забезпечення інформаційної безпеки.

У результаті в США сформувалась теорія національної безпеки і відповідний термінологічний апарат, що лежить в основі документів діючої адміністрації США [2 с. 68–69].

Так як США в XX столітті стали лідером у розвитку інформаційних технологій, соціально-економічні, воєнні та політичні наслідки інформаційної революції стали найбільш відчутними в цій державі. Америка раніше за інші країни зіткнулася з інформаційними загрозами національної безпеки. В результаті цього США стали першими, хто розпочав розробки державної політики у сфері інформаційної безпеки. В США була створена система державного регулювання в інформаційній сфері, що забезпечує ефективне використання сучасних інформаційних технологій для прискорення американської економіки. Разом з тим, питання інформаційної сфери у XX–XXI століттях зайняло одне з провідних місць у державній політиці забезпечення національної безпеки в США.

Американська модель, запропонована у 1993 році як президентська стратегія США, покладена в основу всіх існуючих моделей формування інформаційного суспільства. План дій адміністрації США в сфері Національної інформаційної інфраструктури (The National Information Infrastructure: Agenda for action, 1993) став найважливішою ініціативою адміністрації Клінтона – Гора [3].

Позицію Конгресу США щодо національної інформаційної політики викладено в доповіді Ф. Вайнгартена “Удосконалення федеральної інформаційної політики: погляд Конгресу” (1996 р.), де зазначається, що Сполучені Штати сприймають інформаційні проблеми як політичні чинники для прийняття рішень, що невід’ємні від глобальних проблем американського суспільства. Інформація є одним із основних ресурсів держави, а системи, покладені в основу її створення, обробки і поширення, сприяють прогресивному розвитку і становлять основні соціальні інфраструктури суспільства. Інформаційна індустрія розглядається як головний стратегічний чинник конкуренції та провідний сектор економіки країни.

Інформаційна політика охоплює широке коло урядових заходів: спрямованих на створення інформаційних технологій та управління ними; пов’язаних з потоками інформації; пов’язаних із впливом інформаційних технологій і потоків інформації на конкретні установи чи сферу суспільної діяльності.

Одним із ключових напрямів розвитку інформаційної безпеки, також як і в інших державах, є забезпечення національної безпеки, а саме безпеки інформаційних систем “силових” відомств: воєнних сил, зовнішньої розвідки та ін. Починаючи з 1992 року, основні зусилля по організації заходів у сфері інформаційної безпеки розпочинались Міністерством оборони США в рамках концепції “Інформаційного протиборства”, що орієнтована на вирішення завдань боротьби з системами управління воєнними силами супротивника на різноманітних рівнях і забезпечення безпеки та ефективності своїх інформаційних систем армії США. Подальший розвиток ця концепція отримала в 1996 році у вигляді польового статуту армії США “Інформаційні операції”.

В цілому ж початком сучасної цілеспрямованої систематичної організаційної діяльності у сфері інформаційної безпеки на національному рівні можна вважати директиви адміністрації Президента Білла Клінтона Presidential Decision Directive 63 (PDD 63) “Захист критично важливої інфраструктури” 1998 року. На цьому документі базується підписаний Б. Клінтоном на початку 2000 року “Загальнонаціональний план захисту інформаційних систем”, який визначає основні напрями діяльності держави та всього суспільства у сфері забезпечення інформаційної безпеки.

Також у лютому 2003 року адміністрацією Джорджа Буша-молодшого була опублікована “Національна стратегія досягнення безпеки в кіберпросторі” (“National Strategy to Secure Cyberspace”), в якій п’ять пріоритетів діяльності США по забезпеченню інформаційної безпеки та основних завдань у рамках цих пріоритетів на середньострокову та довгострокову перспективу.

Фактично дані документи можуть вважатися офіційною загальнонаціональною політикою США у сфері інформаційної безпеки, на основі якої будується система діяльності державної влади у цій сфері та структура державних органів, які забезпечують інформаційну безпеку в державі.

Відповідно до стратегії інформаційної безпеки, основними державними пріоритетами у цій сфері є:

1. Становлення та розвиток національної системи реагування на події у сфері інформаційної безпеки.

2. Реалізація комплексної системи заходів по зменшенню загроз інформаційної безпеки.

3. Забезпечення підготовки спеціалістів у сфері комп'ютерної безпеки та відповідального відношення всього населення до питань захисту інформації.

4. Забезпечення захисту інформаційних систем, які мають відношення до державних органів.

5. Розвиток різних форм кооперації (у тому числі й міжнародних) у сфері забезпечення інформаційної безпеки [4].

Пріоритетами національної інформаційної політики США визначено: підтримку досліджень і розробок у галузі інформації і комунікації; вплив на їхнє спрямування та заохочення до поширення технічних знань і можливостей в економіці; сприяння обміну технологіями між лабораторіями та фірмами, запровадження нововведень на ринках; побудову та вдосконалення інформаційної інфраструктури, контроль за її діяльністю, побудову глобальних систем комунікації і дослідження впливу систем на міжнародні, національні та приватні пріоритети; збереження порушеної новими технологіями рівноваги між чотирма основними інформаційними цінностями: конфіденційність інформації, інформацію як суспільне благо, інформацію як товар, інформацію як невіддільний компонент існування держави (необхідне відновлення цієї рівноваги і встановлення нових засобів контролю для нових інформаційних відносин); недоторканність приватного життя, конфіденційність інформації приватного характеру на різних рівнях і в різних сферах державного управління та в приватному секторі; творення урядової політики в галузі інформації і комунікації [3, с. 24–25].

Політика американської держави в інформаційній сфері при адміністраціях У. Клінтона і Дж. Буша була спрямована на формування і зміцнення системи забезпечення інформаційної безпеки США. Ця система продовжує розвиватися і включає в себе законодавчу основу, що забезпечує органи державної влади великими повноваженнями в інформаційній сфері, організаційні структури, до функцій яких входить протидія інформаційним за-

грозам, розслідування інформаційних злочинів, використання інформаційних технологій для забезпечення позицій США на міжнародній арені.

Американська політика у сфері інформаційної безпеки має за мету досягнення, а потім – закріплення домінування США в глобальному інформаційному просторі. Враховуючи велике значення інформаційних ресурсів практично в усіх сферах безпеки, інформаційне домінування є важливим аспектом технологічного, економічного, воєнного і політичного домінування (переваги) США над іншими державами.

Політика США у сфері інформаційної безпеки поєднує як ринкові інструменти лібералізації і регулювання інформаційної сфери, так і намагання встановити прямий державний контроль над інформаційними ресурсами не тільки в національних, а й міжнародних масштабах. У деякому розумінні ці напрями суперечать один одному. Політика лібералізації інформаційної сфери включала такі механізми, як розсекречування воєнних технологій, їх застосування в громадській сфері, зняття заборон щодо експортного контролю, податкові пільги. Американська держава намагалась стимулювати та створювати сприятливі умови для розвитку інформаційного сектору економіки. В той же час використовувались деякі механізми державного політичного контролю через створення стандартів у інформаційній сфері, регулювання застосування комерційних технологій в органах державної влади, а також використання приватних компаній для розвідувальної та контррозвідувальної діяльності.

Адміністрація У. Клінтона спочатку більше звертала увагу на кримінальні аспекти інформаційної безпеки – інформаційні злочини, інші правопорушення із застосуванням інформаційних технологій. Це було обумовлено тим, що центром системи забезпечення інформаційної безпеки у 1990-ті роки було ФБР та Міністерство юстиції США. У другий термін перебування у владі адміністрації Клінтона, суттєво зросла роль воєнних аспектів політики США в інформаційній сфері. Реформа цієї системи при адміністрації Дж. Буша була спрямована на включення в процес забезпечення інформаційної безпеки воєнних і розвідувальних органів. Центральним елементом у цій системі стало створення у 2003 році Міністерства внутрішньої безпеки, воєнні та інші розвідувальні органи мали значні повноваження у цій сфері.

Виступаючи перед працівниками Центрального розвідувального управління в штаб-квартирі ЦРУ в Ленглі, Президент США Джордж Буш назвав головні загрози безпеці Сполучених Штатів – на другому місці, після тероризму, в цьому переліку він зазначив інформаційну війну, і вже за нею – поширення зброї масового ураження і засобів її доставки.

Як вважають американські військові фахівці, до порядку денного поставлене питання про перенесення акценту в збройному протистоянні з традиційних його форм ведення (вогонь, удар, маневр) в ін-

формаційно-інтелектуальну й інформаційно-технічну сфери, тобто туди, де ведеться підготовка, відбувається прийняття і реалізація воєнних і політичних рішень. Майбутня війна може бути спровокована в інформаційній сфері й охоплюватиме всю сукупність завдань у політичній, економічній, технічній і воєнній галузях [3, с. 37].

Одночасно з переходом від постіндустріального до інформаційного суспільства нового значення набуває і споконвічна боротьба щита і меча, броні й снаряда. Полею бою в конфліктах XXI століття стає віртуальний кіберпростір, у якому розгортаються дії інформаційних воєн, а процеси глобалізації накладають певний відбиток і на модернізацію основних концепцій воєнної стратегії XXI століття, що переконливо підтверджує побудова нової національної воєнної стратегії США.

Низка офіційних документів, таких як доповідь Міністерства оборони США “Report of the quadrennial Defense Review”, концептуальний документ Комітету начальників штабів “Joint Vision 2010”, доповідь комісії з національної оборони “Transforming Defense National Security in the 21st Century, Report of the National Defense Panel” констатують відповідно: “Ми визнали, що світ продовжує швидко змінюватися. Ми не в змозі цілком зрозуміти чи передбачити проблеми, що можуть виникнути у світі за часовими межами, зумовленими традиційним плануванням. Наша стратегія приймає такі невизначеності й готує збройні сили таким чином, щоб справитися з ними”; “Прискорення темпів змін робить майбутні умови більш непередбачуваними і менш стабільними, висуваючи широкий діапазон вимог до наших сил”; “Проблеми XXI століття будуть кількісно та якісно відмінними від тих, котрі були характерні для періоду “холодної війни”, у зв’язку з чим виникне потреба докорінної зміни інститутів національної безпеки, воєнної стратегії і підходів до питань оборони до 2020 року” [3, с. 37–38].

Одним із перших кроків влади адміністрації Б. Обама у 2009 р. стала ревізія всієї системи забезпечення інформаційної безпеки в США.

Адміністрація президента Б. Обама почала створювати нову централізовану систему забезпечення інформаційної безпеки США. Створюється новий державний механізм, до функцій якого входить координація всіх зусиль по забезпеченню інформаційної безпеки США.

Найважливішим аспектом у політиці адміністрації Б. Обама у сфері забезпечення інформаційної безпеки є більш тісне співробітництво держави і бізнесу, що спрямоване, в першу чергу, на захист державних інформаційних ресурсів, а також всього американського інформаційного простору. Для цього необхідно втручання американської держави в інформаційну сферу, в тому числі в інформаційний сектор економіки.

Американський досвід державної політики у сфері інформаційної безпеки може бути актуальним для багатьох питань української зовнішньої та внутрішньої політики. Насамперед, необхідно звернути увагу на такі ас-

пекти американського досвіду в сфері забезпечення інформаційної безпеки як: найбільш ефективний підхід до регулювання ринку інформаційних технологій в умовах ринкової економіки. Україна має достатній потенціал для того, щоб бути повноправним учасником інформаційного суспільства. Зазначимо, що ефективність державної політики має не менш важливу роль, у порівнянні з рівнем технологічного розвитку.

Хоча відставання України від світових лідерів у інформаційній сфері в останні роки скорочується, зберігається наша залежність від іноземних інформаційних технологій та програмного забезпечення. Це створює суттєву загрозу національній безпеці України.

Україні, як і іншим державам, необхідно виробити виважену політику держави в цій сфері. Тому, саме досвід США у сфері забезпечення інформаційної безпеки надзвичайно важливий.

Також важливими у забезпеченні інформаційної безпеки є воєнні і розвідувальні аспекти. Досвід США представляє зацікавленість у сфері розвитку воєнних і розвідувальних технологій не тільки всередині ВПК, але й у питаннях державного стимулювання та підтримки інформаційних комерційних технологій. Особливо важливим є американський досвід використання інформаційних технологій для створення систем зв'язку та військового управління, а також високоточної зброї.

Необхідно зазначити, що інформаційна безпека може стати одним із основних напрямів взаємовигідного співробітництва між Україною та США [5].

У відповідності із генеруванням доктринальних положень в США формується і виконавча система, перш за все система державного управління, що відповідальна за зовнішньополітичний курс та забезпечення безпеки держави в цілому, так і на одному з найбільш важливих напрямів забезпечення інформаційної безпеки. Паралельно з нею розвиваються структури та визначене коло обов'язків недержавної системи забезпечення інформаційної безпеки як складової національної безпеки.

У 2002 році було прийнято Закон "Про внутрішню безпеку", відповідно до якого систему забезпечення національної безпеки США було доповнено Міністерством внутрішньої безпеки, а також Радою внутрішньої безпеки, що увійшла до складу адміністрації президента.

До структурних підрозділів Міністерства внутрішньої безпеки відносяться:

Управління прикордонної та транспортної безпеки;

Управління з надзвичайних ситуацій;

Управління науки та технологій;

Управління аналізу інформації та захисту критично важливих національних інфраструктур у складі: Федерального центру захисту від комп'ютерних інцидентів, національної системи зв'язку (Міноборони),

Центру по захисту національної інфраструктури (у складі ФБР), програми захисту енергетичної системи (Міненерго).

Важливу роль у забезпеченні діяльності як системи забезпечення національної, інформаційної безпеки, так і внутрішньої безпеки відіграє ЦРУ, яким керує директор ЦРУ, що спирається на Національну раду з розвідувальної інформації.

Окремі напрями політики забезпечення національної безпеки США реалізуються за рахунок залучення недержавної системи забезпечення національної безпеки [2, с. 432].

І ще один важливий аспект, який не можна не порушити, це щорічне збільшення фінансування забезпечення інформаційної безпеки США, що обраховується сотнями мільйонами доларів США.

У період з 1967 року до сьогодні в США прийнято цілу низку законів, що створюють основу для формування та проведення єдиної державної політики забезпечення інформаційної безпеки з урахуванням інтересів національної безпеки держави. Це закони “Про свободу інформації” (1967 р.), “Про таємницю” (1974 р.), “Про право на фінансову таємницю” (1978 р.), “Про доступ до інформації про діяльність ЦРУ” (1984 р.), “Про комп’ютерні зловживання та шахрайство” (1986 р.), “Про безпеку комп’ютерних систем” (1987 р.) та інші [6, с. 245].

Необхідно визнати, що забезпечення інформаційної безпеки в Україні, насичення держави новими технологіями, розвиток приватного бізнесу тощо відбувається поки що при мінімальному нормативно-правовому забезпеченні.

Для порівняння в США сфера інформаційних та інших технологій, сфера руху інформації регламентується більше, ніж 300 законами та підзаконними актами. Разом з тим сфера інформації вийшла на перший план у сфері національної безпеки, тому що роль та значення інформації швидко збільшились у сучасному світі. При цьому, необхідно відмітити, що акцент у проблемі інформаційної безпеки, окрім прийняття окремих законів, усе більше переміщується в сторону того, наскільки рішення, що приймаються у сфері політики, економіки, науки і технологій будуть, по-перше, відповідати поставленим завданням і, по-друге, наскільки ці рішення будуть адекватними економічним і політичним ситуаціям, що швидко змінюються [7, с. 70–71].

Виходячи з вищенаведеного, можемо зробити логічний висновок, що в США вже сформувалась система забезпечення інформаційної безпеки. Основні елементи єдиного інформаційного простору США, а саме національні інформаційні ресурси, інформаційна інфраструктура, що включає інформаційну інфраструктуру функціонування інформаційного простору, інформаційно-телекомунікаційні структури, що

включають комп'ютерні мережі, інформаційні технології, системи ЗМІ тощо вже сформовані.

Тому відставання України від високорозвинених держав ще раз підкреслює надзвичайну актуальність дослідження проблем забезпечення інформаційної безпеки.

Список використаних джерел

1. Деньщиков А. Л. Информационная стратегия США (анализ, современность, перспективы) : автореф. дис. на соискание учен. степени канд. юрид. наук : [Электронный ресурс] / А. Л. Деньщиков. – Режим доступа : <http://rudocs.exdat.com>.
2. Логунов А. Б. Региональная и национальная безопасность : учеб. пособ. /А. Б. Логунов. – М. : Вузовский учебник, 2009. – 432 с.
3. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : дис. на здоб. наук. ступеня доктора політ. наук : спец. 23.00.02. / Олександр Васильович Соснін ; Одес. нац. юрид. акад. – О., 2005. – 264 с.
4. Общая политика США в сфере информационной безопасности / [Електронний ресурс]. – Режим доступа : <http://www.INTUIT.ru>.
5. Шариков П. А. Политические проблемы международных отношений и глобального развития : автореф. дис. ... канд. полит. наук. / П. А. Шариков. – М., 2004. – 20 с.
6. Туманова Л. В. Обеспечение и защита права на информацию / Л. В. Туманова, А. А. Снытников. – М. : Городец-издат, 2001. – 345 с.
7. Волковский В. И. Экономическая безопасность и информация / В. И. Волковский // Информационная безопасность России в условиях глобального информационного общества : Инфофорум-4 : сб. мат-лов 4-й всерос. конф. – М., 2002. – С. 70–71.

В статье проанализировано состояние и современные тенденции обеспечения информационной безопасности США.

The article analyzes the informational security of USA.

Стаття надійшла до редакції журналу 29 березня 2012 року.