

Кириченко І.\*

## СТРАТЕГІЧНІ ІМПЕРАТИВИ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АДМІНІСТРАЦІЇ Б.КЛІНТОНА

*В этой статье исследуются особенности информационного развития и роли военного сектора США в достижении информационного могущества государства и вывода США на арену международных отношений как наиболее сильного политического, экономического и военного актора, а также оценка государственного видения лидерства США в сфере информационной безопасности.*

**Ключевые слова:** информационная безопасность, информационно-коммуникационные технологии, США, Администрация Билла Клинтона.

*У цій статті досліджуються особливості інформаційного розвитку та ролі військового сектору США у досягненні інформаційної могутності держави та виводу США на арену міжнародних відносин як найбільш сильного політичного, економічного та воєнного актора, а також оцінка державного бачення лідерства США в сфері інформаційної безпеки.*

**Ключові слова:** інформаційна безпека, інформаційно-комунікаційні технології, США, Адміністрація Білла Клінтона.

*The features of information development and the role of the U.S. military sector in building the information capacity of the country and making the United States in the most powerful political, economic and military actor of international relations, the evolution of state vision of U.S. leadership in information security as an example of Clinton administration was studied in article.*

**Key words:** information security, information-communication technologies, USA, Bill Clinton's Administration.

Бурхливий розвиток технологій у другій половині ХХ століття призвів до кількісних і якісних зрушень у сфері інформації та комунікації, що, в свою чергу, суттєво вплинуло на міжнародну систему підтримання миру і стабільності. Вже на межі ХХ і ХХІ століть стало зрозумілим, що науково-технологічні зрушення спричинили збільшення залежності розвитку людини від інформації та ІКТ, які швидко проникали у всі сфери життєдіяльності спільноти. Відтепер потенціал акторів міжнародних відносин почав визначатися категоріями науково-технологічного прогресу та руху інновацій, що також вплинуло на систему безпеки та стратегії її забезпечення на різних рівнях міжнародного співробітництва. Стало зрозумілим, що навмисний або випадковий вплив на інформаційні ресурси або елементи інформаційної інфраструктури може обернутися серйозною загрозою національній безпеці держави або безпеці особистості і суспільства. А отже інформаційна

\* аспірантка Інституту світової економіки і міжнародних відносин НАН України  
Науковий керівник: проф. Макаренко Є.А.

революція значно ускладнила проблему забезпечення інформаційної безпеки. Потужний вплив інформаційної революції на різні соціальні, економічні, політичні, міжнародні та інші процеси пов'язаний з таким феноменом, як інформаційне суспільство, яке формується на всіх рівнях міжнародного співробітництва і об'єднує акторів міжнародних відносин за допомогою інформаційних технологій.

В сучасних умовах розвитку цивілізації істотну роль у забезпеченні безпеки суспільства і держави відіграє інформаційний потенціал. Серйозною проблемою, що виникає у зв'язку з використанням інформаційних технологій є їх подвійна природа і недосконалість норм міжнародного права, які практично не регулюють використання інформаційних технологій у військовій сфері, хоча й визнають інформаційний потенціал одним з визначальних елементів воєнної потуги. Найбільш розвинені держави використовують його для досягнення військових, політичних і економічних цілей. Інструментами інформаційного впливу, таким чином, стають інформаційні ресурси - інформація і технології. Другим важливим аспектом виступає природа глобального інформаційного простору, в якому практично не існує ніяких кордонів, що робить контроль за переміщенням ідей, знань та технологій майже неможливим. Тим не менш, в інформаційному протиборстві перевага буде у тієї сторони, яка зможе досягнути інформаційної переваги - панування в інформаційному просторі космічних систем і засобів розвідки, запобіганні, навігації, метеорології, в управлінні зв'язком. В цьому контексті слід відзначити особливу роль Сполучених Штатів Америки як одного з найбільш могутніх та впливових політичних, економічних і військових акторів сучасних міжнародних відносин. Досягнути такого статусу американській державі вдалося переважно завдяки активному розвитку і впровадженню інформаційних технологій у різні сфери суспільного життя. Після завершення «холодної війни» інформаційний чинник став важливою складовою американського глобального домінування на рівні з військовим та економічним. Водночас, саме США одними з перших зіткнулися й з негативними наслідками інформаційної революції, що дозволило узагальнити досвід протидії інформаційним загрозам державного керівництва країни за останні кілька десятиріч. Тому дослідження цього досвіду є актуальним для розуміння процесів глобалізації комунікації, впливу інформаційних технологій, розвитку інформаційного суспільства та врахування цього досвіду в українській стратегії інформаційної безпеки.

Отже об'єктом дослідження виступає політика США у сфері забезпечення інформаційної безпеки як у внутрішній політиці, так і в міжнародних відносинах, а предметом – політичні, економічні, правові, дипломатичні та військові питання, пов'язані із забезпеченням інформаційної безпеки США. Наукова новизна дослідження визначається тим, що досліджувані питання переважно є принципово новими і відносяться лише до сучасного етапу розвитку міжнародних відносин, а також тим, що питання інформаційної безпеки розглядаються як один з найбільш актуальних напрямків у забезпеченні національної безпеки Сполучених Штатів. Дослідження теми інформаційної безпеки США переважно представлені загальними роботами у сфері геополітики, зовнішньої та безпекової політики США (Ф.Бервелла, І.Даалдера, Б.Блера, Зб.Бжезинського, Ф.Закарії, Г.Моргентау, Е.Картера, У.Перрі, Дж.Стейнбрюннера, Ф.Фукуяма, С.Хантінгтона, І.Іноземцева, П.Циганкова та ін.), а також розробками у сфері інформаційного протиборства (Дж.Ная-мол., М.Лібіцкі, Р.Шафранські, Дж.Стейна, І.Панаріна, В.Лисичкіна, Л.Шелепіна, В.Сліпченка, Г.Почепцова, О.Литвиненка, О.Сосніна та ін.), але питання стратегії інформаційної безпеки США у дослідженнях висвітлені фрагментарно.

Політика інформаційної безпеки США бере свій початок у 1970-80-х рр. і тісно пов'язана зі стрімким зростанням інформаційних технологій та швидким їх впроваджен-

ням у всі сфери життєдіяльності американської спільноти. Внаслідок насичення (задоволення) попиту на промислові товари суспільство стало пред'являти підвищені попит на послуги, що призвело до зростання долі населення, зайнятого у сфері послуг. У середині 70-х рр. ХХ ст. статистичні данні показали якісний стрибок у самій сфері послуг за рахунок широкого впровадження нових ІКТ переважно у такі сфери, як зв'язок, розваги, юридичні та банківські послуги, консалтинг та управління капіталами. Формується сфера інформаційних послуг і по критерію частки зайнятих (т.т. понад 50%) США вже у 1974 р. перейшли до ери інформаційного суспільства [1].

У 1980-90-х рр. розпочинається новий етап у розвитку ідей постіндустріалізму або інформаціоналізму. Перш за все, це пов'язано з тими змінами, які відбулися в розвитку сучасної індустріальної цивілізації. Зокрема в 1991 р. в США вперше витрати на придбання інформації і інформаційних технологій перевищили витрати на придбання виробничих технологій і основних фондів. Зростання обсягів інформаційної складової був настільки стрімкий, що до початку 1995 р. в американській економіці близько трьох чвертей доданої вартості всього промислового виробництва створювалося за допомогою інформаційних технологій. У тому 1995 р. загальна кількість придбаних у США комп'ютерів (16,5 млн. од.) вперше перевищила кількість придбаних автомобілів та телевізорів [2].

За часів адміністрації Б.Клінтона держава активно сприяла розвитку американського інформаційного потенціалу, і до кінця правління президента, Сполучені Штати накопили значний економічний і військовий потенціал, стали найбільш могутньою державою в світі за основними показниками. Одночасно з розвитком інформаційних технологій та їх впровадженням та використанням у різних сферах діяльності американського суспільства, ускладнювалися й загрози інформаційної безпеки. Вже в середині 1990-х років американський уряд звернуло увагу на зростаючу кількість злочинів, скоєних за допомогою інформаційних технологій. Виявилися потенційно уразливості економічної та військової безпеки Сполучених Штатів в інформаційній сфері. Керівництво країни почало розробляти різні способи протидії інформаційним загрозам [3].

Економічне зростання США в 1990-ті рр. багато в чому було обумовлене розвитком інформаційного потенціалу. З розпадом СРСР і зміною геополітичного розподілу сил, Сполучені Штати не тільки залишилися найбільш могутньою державою у світі, а й отримали можливість стати єдиною наддержавою. Після завершення «холодної війни» стратегія Вашингтона була спрямована на консолідацію однополярної системи міжнародних відносин, закріплення позицій США як єдиної наддержави, на досягнення абсолютного американської переваги в світі, що глобалізується.

Вже до початку 1990-х рр. інформаційний потенціал США значно випереджав увесь інший світ. Одним з основних аспектів стратегії глобального домінування було пріоритетний розвиток інформаційного сектору з метою забезпечення технологічного, економічного і військового відриву США від інших акторів міжнародних відносин. Разом з тим у цей період з'явилася низка нових інформаційних технологій (зокрема, Інтернет і мобільна телефонія), які дозволили на якісно новій основі освоїти інформаційний простір [4].

Із завершенням «холодної війни», гостра необхідність у розвитку військових технологій для протидії Радянському Союзу відпала, основним пріоритетом став економічний розвиток, а відповідно і розвиток цивільних технологій, що служили двигуном економічного зростання і джерелом підвищення конкурентоспроможності бізнесу. Нова демократична адміністрація Б.Клінтона внесла багато в чому радикальні пропозиції щодо зміни економічної політики для підвищення конкурентоспроможності країни. У сфері інфор-

маційних технологій пріоритетом державної політики стало не тільки проведення комерціалізації (конверсії) військових технологій, але й використання військовими органами комерційних технологій [1].

У період «холодної війни» військові технології в основному розроблялися за рахунок державного фінансування та були недоступні для комерційного використання. Це вимагало виділення значних коштів з державного бюджету. Розробки технологій цивільного призначення при цьому відбувалися за рахунок приватного капіталу, який у багато разів міг перевищувати розмір державного бюджетного фінансування. Підвищення попиту на інформаційні технології зумовило свого роду об'єднання держави і бізнесу в області розробки інформаційних технологій. Результатом проведеної в США державної економічної політики, спрямованої на стимулювання і активну державну підтримку інформаційних технологій стало формування потужного інформаційно-технологічного комплексу, який складався як з матеріального виробництва, так і сфери послуг. Саме він був одним з рушіїв американської економіки і сприяв досягненню Сполученими Штатами позицій глобального лідерства.

Адміністрація президента Б.Клінтона вперше включила технологічну політику держави до національної стратегії економічного розвитку. Ще під час президентських виборів 1992 р. представники Демократичної партії США стверджували, що інвестиції у розвиток технологій та інфраструктури - запорука економічного процвітання американської держави в майбутньому. Загалом політика адміністрації президента Б.Клінтона була спрямована на максимальне використання цих технологій для того, щоб не тільки прискорити соціально-економічний розвиток США, але і забезпечити глобальне інформаційне лідерство [5].

Першим проектом, ініційованим адміністрацією Б.Клінтона у 1993 р., став проект «Національна інформаційна інфраструктура» [6], спрямований на розвиток різних секторів американської економіки на основі широкого застосування інформаційних технологій. Основним завданням проекту була інтеграція нових технологій і масштабне поширення компонентів інформаційної інфраструктури в різних галузях промисловості. Проект був призначений для створення механізму швидкого впровадження інновацій та освоєння їх переваг в соціально-економічній сфері.

Іншим напрямком діяльності адміністрації у сфері інформаційно-технологічного розвитку була масована конверсія військових технологій. Однією з головних цілей продуманої конверсії національного науково-технічного потенціалу США було максимальне сприяння прискореному розвитку ІТ-сектору. Зокрема, в 1994 р., міністр оборони У.Перрі випустив директиву, яка дозволила всім видам збройних сил при закупівлі військової продукції та розробці нових систем зброї в обов'язковому порядку використовувати комерційні технічні характеристики, специфікації і стандарти. Відступати від цього правила дозволялося лише з санкції міністра оборони. Більше того, була підготовлена директива про технології подвійного використання: стратегія створення доступних передових оборонних технологій. У цьому документі, зокрема, говориться, що «метою проведеної Міністерством оборони реформи закупівель є створення закупівельної системи комерційного типу, яка орієнтується на комерційні вироби і технології. Така система повинна виключати використання спеціальних контрактних умов і технічних вимог, а також правила звітності, оскільки усе це перешкоджає військово-комерційній інтеграції» [8].

Значним елементом у просуванні американських технологій на світовий ринок була реформа системи експортного контролю Сполучених Штатів. На початку 1990-х рр. були зняті деякі обмеження на експорт суперкомп'ютерів. Всі країни, за винятком країн-ко-

лишніх членів Організації Варшавського договору і Китаю, отримали можливість імпортувати американські комп'ютери, що стимулювало розвиток міжнародної конкуренції серед виробників. З появою конкурентів на міжнародному ринку ефективність реформи експортного контролю швидко зійшла нанівець, і наприкінці 1999 р., практично всі обмеження на експорт суперкомп'ютерів були зняті [1].

Значним кроком у сфері лібералізації та дерегуляції інформаційної сфери Сполучених Штатів була комерціалізація Інтернету. За часів адміністрації Б.Клінтона дії американської держави були спрямовані на те, щоб створити максимально сприятливі умови для розвитку комерційних інформаційних технологій з метою забезпечення економічного зростання. Внаслідок такої політики в Сполучених Штатах суспільство, бізнес і громадяни отримали безпрецедентний доступ до значних інформаційних ресурсів [9].

Такі технологічні зрушення суттєвим чином вплинули на формування системи державного забезпечення інформаційної безпеки адміністрацією Б.Клінтона. Нові можливості, що з'явилися внаслідок розвитку інформаційних технологій, створили для користувачів значні можливості для порушення майнових прав. Як показали проведені дослідження, з'явився істотний розрив щодо правової бази через технічну відсталість правоохоронних органів у порівнянні з можливостями здійснення інформаційних злочинів. Проблема ускладнювалася й тим, що уразливість інформаційної безпеки зростає як в державному і приватному секторі, так і на рівні окремих громадян. Крім того, значна частина державних і економічних підприємств опинилася у жорсткій залежності від використання інформаційних технологій. Найбільш показовим прикладом подібної залежності була «проблема 2000». Деякі фахівці у сфері інформаційних технологій висловлювали побоювання, що всі інформаційні системи вийдуть з ладу 1 січня 2000 через технічні характеристики основних програмних кодів. У цей період у США вперше було усвідомлене посилення залежності від інформаційних технологій. Було офіційно визнано, що інформаційні загрози є серйозною проблемою національної безпеки. Одним з найважливіших напрямків у забезпеченні інформаційної безпеки став захист критично важливих елементів національної інфраструктури, найважливішими з яких було визнано саме інформаційні технології (на рівні безпеки водо- та електропостачання, хімічної промисловості, поштового сполучення, охорони здоров'я, сільського господарства, енергетики тощо) [4].

У 1998 р. президентом Б.Клінтоном було підписано директиву № 63, «Про захист критично важливих елементів національної інфраструктури структури» [10], в якій зазначалося про необхідність та доцільність створення в рамках ФБР Центру захисту національної інфраструктури, до обов'язків якого входило вивчення і попередження про загрози, які з'являються в інформаційному просторі, розслідування кримінальних злочинів, пов'язаних з використанням інформаційних технологій. У структурі кожної державної установи мала бути створена посада директора з інформаційних технологій, який повинен відповідати за інформаційну безпеку свого відомства. Крім того, була започаткована посада радника президента з питань захисту інфраструктури та протидії тероризму. Діяльність Центру із захисту національної інфраструктури мала переважно інформаційний характер, а рекомендації, розроблені центром у сфері протидії інформаційним загрозам, виконувались нерегулярно.

Ще до завершення президентського терміну Б.Клінтона проблеми, пов'язані із забезпеченням інформаційної безпеки, стали серйозною загрозою національній безпеці Сполучених Штатів. Кількість випадків інформаційних злочинів збільшувалася, шкідливі програми вражали елементи інформаційної інфраструктури, частішали випадки незаконного використання прав інтелектуальної власності, розвиток інформаційних технологій дозволив багатьом злочинцям отримувати несанкціонований доступ до конфіденційної,

комерційної інформації і навіть до державної таємниці. Таким чином, питання забезпечення інформаційної безпеки стали пріоритетом у забезпеченні національної безпеки Сполучених Штатів за часів адміністрації Б.Клінтона. При цьому головний наголос було зроблено на закріпленні за допомогою інформаційних технологій лідерства США в економічній і військовій сферах. Крім того, Вашингтон спробував захопити домінуючі позиції в світовому інформаційному просторі. Інформаційні технології були покладені в основу так званої «м'якої сили», на розвиток якої зробила наголос адміністрація Б.Клінтона [11].

Завдяки потужним технологічним зрушенням США у XX столітті стали лідером інформаційного та інноваційного розвитку, а соціально-економічні, військові та політичні наслідки інформаційної революції виявилися найбільш відчутними в цій країні. Сполучені Штати стали першою державою світу, яка серйозно поставилася до проблем національної безпеки, пов'язаних з інформаційно-технологічним розвитком, і включила до стратегії національної безпеки питання інформаційної безпеки як важливого чинника розвитку американського суспільства. Тому безпекова політика американського уряду за адміністрації Б.Клінтона була спрямована на формування та зміцнення всеохоплюючої системи забезпечення саме інформаційної безпеки держави.

Сформована у 1990-х рр. система продовжує сьогодні еволюціонувати і набуває нових ознак і характеристик відповідно до вимог часу та появи нових загроз для системи національної безпеки та оборони. Закладена тоді система продовжує розвиватися і вже містить значну законодавчу базу, що забезпечує органи державної влади значними повноваженнями в інформаційній сфері, організаційні структури, у функції яких входить протидія інформаційним загрозам, розслідування інформаційних злочинів, використання інформаційних технологій для зміцнення позицій США на міжнародній арені.

В американській державній системі забезпечення інформаційної безпеки утворилася унікальна модель державно-приватного партнерства правоохоронних, військових і розвідувальних органів, а також бізнесу: політика США в галузі інформаційної безпеки поєднує як ринкові інструменти лібералізації та дерегуляції інформаційної сфери, так і прагнення встановити прямий державний контроль над інформаційними ресурсами, причому не тільки в національному, але і в міжнародному масштабах. Слід також відзначити, що американська політика у сфері інформаційної безпеки при адміністрації Б.Клінтона мала на меті не тільки створення ефективної системи захисту національного інформаційного простору та інформаційної інфраструктури, а й досягнення, а згодом закріплення домінування США в глобальному інформаційному просторі.

### Список використаних джерел

1. Роговский Е.А. Информационное общество (экономика и политика) / Е.А.Роговский. – М.: Международные отношения, 2008. – 408 с.
2. Роговский Е.А. Лидерство США в глобальных технологиях и международная безопасность / Е.А.Роговский // США и Канада: экономика, политика, культура. – 2007. - №9. – С. 25-37.
3. Информационные вызовы национальной и международной безопасности / [И.Ю.Алексеева и др.]; Под общ. ред. А.В.Федорова, В.Н.Цигичко. – М.: ПИР-Центр, 2001. – 328 с.
4. Шариков П.А. Государственная политика в области информационной безопасности - опыт США и уроки для России / П.А.Шариков // Сборник докладов аспирантов ИСКРАН и студентов ФМП ГУГН на конференции 29 ноября 2006 г. - М.: Институт США и Канады РАН, 2007. - С. 12-21.

5. Шариков П.А. Политика США в области информационной безопасности: автореф. дис. на соискание ученой степени канд. политических наук: спец. 23.00.04 «Политические проблемы международных отношений и международного развития» / Шариков Павел Александрович. – М., 2009. – 33 с.
6. Critical Foundations: Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection [Electronic resource]. – Access mode: [https://www.cerias.purdue.edu/apps/reports\\_and\\_papers/view/2021](https://www.cerias.purdue.edu/apps/reports_and_papers/view/2021).
7. Adams T.K. 10 GPS Vulnerabilities [Electronic resource] / Thomas K. Adams // Military Review. – 2001. – March-April. – Access mode: <http://www.c4i.org/gps-adams.html>
8. Dual Use Technology: A Defense Strategy for Affordable, Leading-Edge Technology. Department of Defense. – Wash: Government Printing Office, February 1995. – P. 16.
9. A Survey of Government and Internet. Digital Democracy // (The) Economist. – 2000. – № 24. – P.24-31.
10. Protecting America's Infrastructures: Presidential Decision Directive 63 (May 22, 1998) [Electronic resource]. – Access mode: <http://www.fas.org/irp/offdocs/pdd-63.htm>.
11. Crabb C.V., Jr. Invitation to Struggle. Congress, the President and Foreign Policy / Cecil.V. Crabb, Jr., Pat M. Holt. – [Fourth Edition]. – Washington, DC: CQ Press, 1992. – 322 p.