УДК 316.324.8:004

Н.Б. Бєлоусова
кандидат політичних наук, доцент кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

КОНЦЕПТУАЛЬНІ ЗАСАДИ СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ США ЗА АДМІНІСТРАЦІЇ БАРАКА ОБАМИ

У цій статті надається стислий опис нової стратегії інформаційної безпеки США, що втілюється в життя адміністрацією Барака Обами, характеризуються її особливості та перспективи. Наводиться реалізація нової стратегії інформаційної безпеки в структурі політичних та соціальних процесів США.

Ключові слова: стратегія, інформаційна безпека, Барак Обама, інформаційна перспектива, структура, процес.

Сучасний етап розвитку людства є переходом до інформаційного суспільства й глобальної інформаційної економіки (економіки знань), коли зникають межі національних і регіональних ринків, зближуються сфери виробництва і споживання, загострюються різноманітні ризики, виклики та загрози, зокрема, пов’язані з боротьбою за обмежені енергетичні, сировинні, фінансові й інтелектуальні ресурси.

Хоча інформація і комунікації завжди були важливими складниками державної зовнішньополітичної стратегії, у сучасному світі йдеться про виникнення якісно нової ситуації, коли «контроль за інформацією», «могутність» і «впливовість» нерозривно пов’язані між собою. У зовнішній політиці управління інформаційними ресурсами перетворилося на життєво важливий атрибут, органічний складник стратегічного планування. Це стосується також усіх без винятку аспектів і вимірів зовнішньої політики (економічного, екологічного, військового тощо).

Виникає нетривіальна ситуація підпорядкованості більшості аспектів зовнішньої політики інтересам національної та міжнародної інформаційної безпеки, значимість яких переконливо довела ухвалена 23 липня 2000 р. Окінавська хартія глобального інформаційного суспільства. У свою чергу, це підтвердив Всесвітній саміт з інформаційного суспільства під егідою ООН, перший етап якого відбувся у грудні 2003 р. в Женеві, а другий - у листопаді 2005 р. в Тунісі. Подібні глобального змісту документи є переконливим доказом того, що здатність країни «вписатись» у координати глобального інформаційного суспільства, невпинно нарощувати свої інформаційні ресурси й ефективно ними керувати є нині найважливішою проблемою національної й міжнародної безпеки. Інформаційна сфера здатна як виступати провідним чинником реалізації найважливіших суспільних проектів, так і перетворюватися на чинник хаотизації й гальмування соціального, економічного й культурного розвитку [3].

Інформаційна «м'яка сила» наразі має істотний пріоритет перед силою традиційною – матеріальною, «грубою», що переконливо довела антитерористична кампанія, яку після трагічних подій 11 вересня 2001 року розгорнули американський президент Джордж Буш та очолювана ним адміністрація, а також невдачі політики американців і їхніх союзників з коаліції в Іраку.

Події 11 вересня 2001 року спонукали США та інші держави світу взяти під контроль інформаційно-комунікативні технології й інформаційний обмін. Відбувається поділ світу на країни інформаційно розвинені та нові, що розвиваються. Посилюється інформаційна нерівність, що більш-менш адекватно відображає терміни «інформаційний імперіалізм» та «інформаційне гетто» тощо [6].

У свою чергу, потребує аналізу й відповідного рівня формалізації та узагальнення досвід, набутий «інформаційно розвиненими» країнами у сфері управління інформаційними

потоками та інформаційними ресурсами за певних зовнішніх і внутрішніх кризових умов. Урахування цього досвіду необхідне для забезпечення ефективнішої політики України як у сфері захисту національного інформаційного простору, так і в царині інформаційної підтримки зовнішньої політики. Ідеться про оптимізацію системи реагування на інформаційні виклики та акції зовнішніх суб'єктів політики з метою забезпечення власного інформаційного суверенітету.

Як відомо, перша країна, що почала інформатизацію, – це США. Інші промислово розвинені країни світу, зрозумівши перспективність і неминучість цього процесу, досить швидко зорієнтувались і почали нарощувати темпи впровадження комп'ютерів та засобів телекомунікацій.

Крім того, США посідають 1-ші місця у світі за встановленою сумарною потужністю комп'ютерів і за комп'ютерною потужністю, розраховуючи на душу населення. Індустрія інформації в США входить у першу десятку пріоритетних галузей економіки, поступаючись лише аерокосмічній, радіоелектронній і фармацевтичній. На розвиток інформатизації в США витрачається близько 2% річних витрат федерального бюджету. США контролюють понад 65% світового ринку комп'ютерів, 63% ринку програмного забезпечення Західної Європи, 54% аналогічного ринку Японії. З десяти найбільших у світі фірм-виробників програмного забезпечення шість – американські. Американським компаніям й університетам належить більша частина світових патентів у сфері інформаційних технологій. Найближчими роками США залишаться найбільшим у світі ринком програмного забезпечення [9].

У середині 1990-х років у США були зосереджені 426 із 816 світових інформаційних банків даних з науково-технічних дисциплін і 716 із 1035 наявних у світі баз даних з економічних дисциплін [9]. США дозволяють собі «поступатися позиціями» у будь-якій сфері діяльності (допускати на свій ринок товари з

Японії тощо), але не у виробництві знань. США мають максимум кваліфікованого населення – населення, здатного пристосовуватися до нових технологій (здійснювати рецепцію, трансферт технологій) за рахунок рівня освіти.

Інформаційна зовнішньополітична стратегія, одночасно з військовим, економічним та іншими чинниками, є найважливішим складником розв'язання кризових проблем у сучасній міжнародній системі. Під «інформаційною стратегією» слід розуміти засадничу модель гнучкого застосування інформаційних зовнішньополітичних підходів, спрямованих на захист вітчизняного інформаційного простору та ефективне забезпечення національних інтересів на міжнародній арені.

Цілі стратегічного інформаційного протистояння із використанням глобального інформаційного простору для реалізації імперативів зовнішньої політики визначаються характером політичних та військових конфліктів, заради розв'язання яких проводиться боротьба, а новітні інструменти інформаційної стратегії мають ту специфіку, що не сприймаються як загрозливі не лише населенням, але й політичними елітами країн-мішеней.

Епоха терору й антитерору призвела до появи нових видів інформаційної зброї (листи з «підозрілою речовиною», «сигнали» щодо вчинення терористичних актів тощо), які не лише деструктивно впливають на стани масової свідомості, політичну й економічну ситуацію в окремих країнах та світі в цілому, але й руйнують знаково-символьну інфраструктуру «нового» глобального мислення, заснованого на загальнолюдських цінностях [5].

Антитерористичні операції обумовили низку новітніх тенденцій в інформаційному забезпеченні зовнішньополітичного курсу адміністрації президента США Джорджа Буша; переформатування внутрішніх і зовнішніх інформаційних потоків; запровадження нових моделей комунікацій між владою, засобами масової інформації та

масовою аудиторією; використання слоганів демократії та прав людини для реалізації курсу «демократичного імперіалізму».

У сучасному світі прогрес неможливий без опори на цифрову інфраструктуру – наріжний камінь, що лежить в основі процвітання економіки, сильної армії, відкритого й ефективного уряду. Уже багато разів говорилося про те, що революція у сфері комунікацій та інформаційних технологій породила якийсь віртуальний світ. Але не будемо помилятися: у реальності ми залежимо від кіберпростору кожен день. Він включає все наше обладнання та програми, настільні й портативні комп'ютери, мобільні телефони, які вплетені в тканину кожного аспекту нашого повсякденного життя. Це широкосмугові та бездротові мережі, локальні мережі в школах, лікарнях, на підприємствах, інші масові мережі, які служать країні. Це і секретні військові і розвідувальні мережі, і відкритий Веб, який пов'язав людей сильніше, ніж будь-коли в історії людства. Отже, кіберпростір реальний. Звідси реальні і ризики, які прийшли разом з ним.

У цьому полягає велика іронія нашої інформаційного епохи – ті ж технології, що дозволяють нам створювати і будувати, дають новий шанс для тих, хто хоче нам нашкодити. Цей парадокс - видимий і невидимий - це те, що ми відчуваємо щодня. Мова ідеться про приватне життя економічну безпеку американських сімей. Ми розраховуємо на Інтернет, оплачуючи рахунки, в банках, магазинах, при оплаті податків. Але потрібно знати цілий словник термінів для того, щоб бути на крок попереду кібер-злочинців, їх шпигунських і шкідливих програм, спуфінгу, фішингу та ін. [7]. Мільйони людей уже стали їх жертвами: їх приватне життя порушується, їх особисті дані викрадаються, їх гаманці спорожняються і все життя перевертається догори дном. За даними дослідження групи AIG, тільки за останні два роки кіберзлочинність коштувала американцям 8 млрд. доларів [12]. У період між серпнем і жовтнем 2008 року хакери здобули доступ до електронної

пошти і низки файлів передвиборної кампанії Барака Обами, включаючи документи, що розкривають політичні позиції та плани поїздок. Штабістам довелося тісно співпрацювати з ЦРУ, ФБР і Внутрішньої Службою безпеки, наймати консультантів для відновлення наших систем [12]. Це стало серйозним нагадуванням: в інформаційний вік ваша ключова перевага - а в цьому випадку це була можливість спілкуватися з широким колом прихильників через Інтернет - може стати найслабшою ланкою. Минулого року одним цинічним актом злодії вкрали мільйони доларів з 130 банкоматів в 49 містах по всьому світу, використовуючи викрадені з кредитних карт дані. І вони зробили це всього за 30 хвилин. Співробітник американської компанії Intel звинувачується у крадіжці інтелектуальної власності на суму 400 млн. доларів. За оцінками за минулий рік, по всьому світу кібер-злочинці вкрали інтелектуальної власності на суму до $ 1 трлн [17]. Економічне процвітання Америки в XXI столітті буде залежати від кібербезпеки. Тепер очевидно, що кіберзагроза – це одна з найсерйозніших економічних і національних проблем цієї держави.

Ясно також, що США належно не підготовлені до таких загроз ні в уряді, ні в державі. Останніми роками був досягнутий певний прогрес на федеральному рівні. Але так само, як США провалювали інвестування у «фізичну» інфраструктуру – дороги, мости та залізниці – так проґавили і необхідність вкладень у безпеку цифрової інфраструктури.

У США немає жодного офіційно відповідального з нагляду за політикою кібербезпеки у федеральному уряді – жодна установа не несе відповідальності і не має повноважень, що відповідають складності та масштабу цієї проблеми. Насправді, коли йдеться про кібербезпеку, федеральні органи багато в чому навіть перекривають свої функції, але обміну інформацією і координації дій один з одним і з приватним сектором немає. Ми спостерігаємо це, наприклад, у відсутності організованої відповіді на появу вірусу Conficker – мережевого

«хробака», що заразив за місяці мільйони комп'ютерів у всьому світі [13].

Щоб надати цьому починанню належний рівень представництва і фокус, якого вона заслуговує, у травні 2009 року оголошена організація Єдиної Ради з Національної Безпеки. У Білому Домі створюється новий відділ, яким буде керувати Координатор з кібербезпеки [14]. З огляду на виняткову важливість цієї сфери, Барак Обама візьме особисту участь у виборі цієї посадової особи. Він розраховує на цей відділ у всіх питаннях, пов'язаних з кібербезпекою, і його керівник матиме його повну підтримку. Слід підкреслити важливість функцій, які виконуються на цій посаді: це – інтеграція і злагоджена робота всіх аспектів політики кібербезпеки в галузі управління; тісна співпраця з офісами Білого Дому, щоб бюджет агентства відбивав його пріоритети, а також координація дій у відповідь у випадку великих подій або нападів.

Для федерального складника політики зміцнення інформаційної безпеки, координатор з кібербезпеки також буде членом Ради Національної безпеки, а також членом Національної економічної ради. Щоб забезпечити відповідність цієї політики Ради американським основоположним цінностям, у нього будуть включені посади, які займаються охороною громадянських свобод і особистого життя американського народу.

У своїй доповіді від 29 травня 2009 року Обама означив п'ять головних напрямів діяльності [15]:

«По-перше, працюючи в тісній співпраці з громадами, представленими тут сьогодні, нам належить розробити нову всеосяжну стратегію щодо забезпечення безпеки інформаційно-комунікаційних мереж Америки. Щоб посилити зв'язок з федеральними агентствами, кібербезпека буде одним з моїх ключових пріоритетів.

Друге. Забезпечити єдину і організовану відповідь на кібератаки ми можемо тільки працюючи спільно – зокрема з державними та місцевими органами влади, приватним сектором. Необхідно реагувати так само, як ми реагуємо на стихійні лиха – потрібно заздалегідь мати готові плани і ресурси, обмінюватись інформацією, видавати попередження і забезпечувати скоординовані заходи у відповідь.

Третє. Ми будемо зміцнювати співробітництво державного та приватного секторів, що має вирішальне значення в цьому починанні. Переважна більшість найважливіших інформаційних інфраструктур у США перебуває у власності або управляються приватним сектором.

Четверте. Ми будемо продовжувати вкладати кошти в передові дослідження і розробки. Це необхідно, щоб зробити відкриття, які будуть відповідати цифровим викликам нашого часу.

І, нарешті, ми почнемо національну пропагандистську кампанію з метою повсюдного усвідомлення даної проблеми, інформованості і грамотності у сфері цифрових технологій»

Про початок епохи «гонки озброєнь» у кіберпросторі оголосив глава компанії-розробника антивірусних програм McAfee Дейв ді Велт під час Всесвітнього економічного форуму в Давосі в січні 2010 року. За його словами, останнім часом спостерігається рух державних комп'ютерних структур від традиційних оборонних стратегій до наступальних. Інтернет стає полем міжнародних бойових дій. Півтора-два десятки країн, серед яких Росія, США та Китай, готуються до можливих операцій в Інтернеті. Експерти вже закликають до активного публічного обговорення проблеми віртуальних воєн [10].

Фахівці McAfee виявили ознаки застосування «кіберзброї» принаймні в п'яти країнах – США, Китай, Росія, Ізраїль та Франція. І цей список буде розширюватися. «Зараз ми бачимо понад 20 країн; уряди яких озброюються, готуючись до

кібервійни, кібершпигунства, нарощуючи кібернаступальний потенціал», – заявив ді Велт.

Ці дані були представлені ще восени 2009 року в черговій доповіді McAfee «Звіт про віртуальну злочинність». Раніше про ризик розвитку наступальних видів інформаційних технологій попереджав голова Міжнародного телекомунікаційного союзу при ООН Хамадун Туре [16].

У цілому, останнім часом відзначається різке збільшення кількості хакерських атак в усьому світі. Зокрема, за підрахунками McAfee, за рік кількість нових шкідливих програм зросло на 500%. Також спостерігається і підвищена увага світової громадськості до кібергалузі. Це наочно демонструє, на думку ді Велта, недавній випадок з компанією Google, яка після хакерської атаки на поштовий сервіс заявила про намір припинити роботу в Китаї. Але це було лише одне з багатьох подібних нападів за останні 12 місяців, більшість же з них пройшли непоміченими для публіки. Тим часом експерти попереджають, що в майбутньому кібератаки проти ключових об'єктів життєзабезпечення, які в більшості розвинених країн недостатньо захищені, можуть обернутися величезним збитком. Вже зараз, як показало дослідження McAfee, атаки хакерів обходяться в середньому в $ 6,3 млн. на добу, тобто в $ 1,75 млрд на рік по всьому світу [8]. Найдорожчі – напади на мережеву інфраструктуру нафтогазового сектора. Антивірусна компанія McAfee спільно з Центром стратегічних і міжнародних досліджень (CSIS) представила на Всесвітньому економічному форумі в Давосі звіт про результати дослідження, проведеного серед шестисот керівників нафтових і газових об'єктів, електростанцій та іншої критично важливої інфраструктури.

Підчас опитування 54% менеджерів вищої ланки вони визнали, що очолювані ними об'єкти вже постраждали від великомасштабних кібератак з боку організованих злочинців, терористів та окремих держав. Гірше того, що 37% респондентів повідомили про те, що минулого року через

скорочення корпоративних бюджетів ситуація з кібербезпекою стала ще гіршою, ніж раніше. Сорок відсотків опитаних очікують в новому році великого інциденту в сфері кібернетичної безпеки. Середня величина прогнозованого збитків від простою, викликаного збоєм у роботі IT-систем, буде перебувати на рівні 6,3 мільйона доларів на день. При цьому 45% керівників вважають, що відповідальність за запобігання таких атак повинні нести регіональні або місцеві органи влади [4].

Щодо глобальної кібербезпеки, поки не існує чітких визначень кібервійни і кіберзброї. Тому неможливо визначити, на якому етапі віртуальні атаки можуть вилитися у військове протистояння, зазначають фахівці, закликаючи до відкритого обговорення проблем кіберзлочинності. Примітно, що деякі експерти пов'язують заяви про кібервійни з комерційними інтересами McAfee, оскільки це могло б привернути увагу до продукту компанії. «Не думаю, що можна всерйоз підозрювати, що, наприклад, в Китаї або в Кремлі сидять люди і планують хакерські атаки на які-небудь країни», – відзначає голова ради АНО «Координаційний центр національного домену мережі Інтернет» Михайло Якушев [6].

Тим часом колишній заступник директора Управління національної безпеки США Вільям Кроуел, навпаки, вважає, що впродовж наступних 20–30 років кібератаки стануть невід'ємною частиною військової стратегії. Як повідомила американський сенатор Сьюзен Коллінз на Давоському форумі, у США всерйоз розглядається питання про прирівнювання кібератаки до оголошення війни. А Хамадун Туре порівняв кібервійни з цунамі, запропонувавши розробити угоду, за якою країни візьмуть на себе зобов'язання не влаштовувати хакерські атаки першими [6].

Щоб запобігти світовій кібервійні, топ-менеджери IT компаній запропонували ввести обов'язковий документ для користувачів – аналог водійських прав. Касперський

запропонував заснувати Інтернет-поліцію, а російська влада хоче видавати email як паспорт. На думку активістів обмеження доступу до мережі, люди звикли проходити ідентифікацію в різних сферах життя, і Інтернет не повинен стати винятком. На Всесвітньому економічному форумі в Давосі генеральний секретар Міжнародного телекомунікаційного союзу Хамадун Туре заявив, що сучасний світ має потребу в договорі, який міг би запобігти прийдешню світову кібервійну. Директор з досліджень і стратегії корпорації Microsoft Крейг Манді як рішення запропонував ввести обов'язковий документ для Інтернет-користувачів – аналог водійських прав. «Проблема в тому, що люди не розуміють масштаби і загрозу злочинної діяльності в Інтернеті», – заявив він [11].

Глава компанії McAfee Девід Деволт заявив, що до ведення кібервійни готові приблизно двадцять країн. Нині всі ці країни займаються активним інтернет-шпигунством у відношенні один до одного. Глава McAfee відзначив, що останні атаки, пов'язані з Китаєм та компанією Google, наочно демонструють ефект перемикання уваги на кібер-галузь. Однак випадок з Google глава McAfee назвав лише верхівкою айсберга. Він розповів, що за останній рік його компанія знайшла кілька надзвичайно витончених кібератак, але про більшість з них публічно нічого не повідомлялося. Випадок з Google став неординарним. Разом з тим, згідно з даними статистики, у загальному обсязі із США виходить близько 36% хакерського трафіку, тоді як з КНР - лише 33%. Китайська ж влада заявила про те, що саме їхня країна є найбільшою в світі мішенню для кіберзлочинців. Таку точку зору висловив, зокрема, Чжоу Юнлінь, заступник оперативного відділу Технічної служби з екстреного реагування на інциденти в комп'ютерних мережах (CNCERT). Крім того, Чжоу Юнлінь повідомив про те, що йому нічого не відомо про атаки, нібито проведені китайськими хакерами на Google. Він заявив, що компанія Google не надала CNCERT ніяких доказів нападу і не зверталася до служби за

допомогою, незважаючи на те, що CNCERT завжди активно співпрацює з американським US-CERT при розслідуванні подібних інцидентів [5].

Отже, хоча інформація і комунікації були важливими складника державної зовнішньополітичної стратегії США за президентства Джорджа Буша-молодшого, у сучасному світі йдеться про виникнення якісно нової ситуації, коли «контроль за інформацією», «могутність» і «впливовість» нерозривно пов'язані між собою. У зовнішній і внутрішній політиці управління інформаційними ресурсами перетворилося на життєво важливий атрибут, органічний складник стратегічного планування. Це стосується також усіх без винятку аспектів і вимірів політики (економічного, екологічного, військового тощо).

Адміністрація Барака Обами заявила, що буде здійснювати новий комплексний підхід до забезпечення безпеки цифрової інфраструктури Америки. Надалі американська цифрова інфраструктура – мережі та комп'ютери − будуть розглядатися так, як вони повинні розглядатися – як стратегічний національний актив. Захист цієї інфраструктури буде пріоритетом національної безпеки.

Отже, впровадження нової стратегії інформаційної безпеки Бараком Обамою у США свідчить про зростаючу роль впливу цієї сфери людської діяльності на забезпечення стабільного функціонування державного апарату в одній з найбільших країн світу.

Література

1. Барак Обама. Дерзость надежды / Барак Обама. – Азбука-классика, 2008 – 145 с.
2. Буткевич М. Курс на Обаму / М. Буткевич // Український тиждень. – №44. – 2009. – С. 26.
3. Вайнгартен Ф. Основи федеральної інформаційної політики: Погляд конгресу США / Ф. Вайнгартен. – 2006. – С. 23.

4. Даниелова А. Основные направления информатизации американского общества / А. Даниелова // США-Канада. – 2009. – №5 – С. 27.
5. Жуков В. Взгляды военного руководства США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение. – 2005. – № 1. – С. 26.
6. Інформаційні технології та тенденції розвитку міжнародної інформації // Вісник книжкової палати – 2010. – №6 – С. 32.
7. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. / В.Д. Курушин, В.А. Минаев. – М.: Новый юрист, 2008. – С. 39.
8. Прохожев А.А., Турко Н.И. Основы информационной войны. Анализ систем на пороге XXI века: теория и практика. / А.А. Прохожев, Н.И. Турко. – М., 1996. –С.45.
9. Роговской Е. Развитие информационного сектора США к началу XXI века / Е. Роговский. – США-Канада. – 2002. – №4. – С.34.
10. Тумарец В. Новые угрозы для информационного общества. / В. Тумарец. – М. : ЭКСМО, 2008. – С. 58.
11. Шершнёв Е. Информатизация общества и экономики США / Е. Шершнёв, США-Канада – 2008. – №1 – С.62.
12. AIG Technology Report 2007-2008: Readiness for the Networked World Center for International Development at Harvard University, March 2009. – P.16
13. America's first peer-to-peer President [Електронний ресурс] // Havas Media. – Режим доступу: http://www.mpg-austria.com/media/pages/havasmediawhite paperobama_doc_343_1.pdf
14. Barack Obama Speech, March, 13, 2009 [Електронний ресурс] / Barack Obama Site. – Режим доступу: http://my.barackobama. com/ page/ content/ofasplashbsignon/
15. Remarks by the President on Securing our Nation's Cyber Infrastructure – [електронний ресурс] // White House Official Site. – Режим доступу: http://www.whitehouse.gov/the_press

_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure
16. United Nations «Global E-Government Survey–2008» [Електронний ресурс] / UN PAN Site. – Режим доступу: http://www.unpan.org/egovkb/global_reports/08report.htm
17. WIPO 2008 Report – [Електронний ресурс] / WIPO Site. – Режим доступу: http://www.wipo.int/meetings/en/archive.jsp

The author of this article describes main components of the new strategy of the information security of the USA realized by Barack Obama's team. Positive and negative factors are presented as well as analyses of the features and outlooks of the new strategy. An implementation of the new strategy of information security in the structure of political and social processes of the United States.

Key words: strategy, information security, Barack Obama, the information perspective, structure, process.

В этой статье дается краткое описание новой стратегии инфомационной безопасности США, которая воплощается в жизнь администрацией Барака Обамы, также характеризуются ее особенности и перспективы. Приводится реализация новой стратегии информационной безопасности в структуре политических и социальных процессов США.

Ключевые слова: стратегия, информационная безопасность, Барак Обама, информационная перспектива, структура, процесс.