зарубіжний досвід

УДК 316.776.23()73

Кібербезпекова політика в контексті трансформації політики безпеки США за адміністрації Б. Обами

Дмитро Дубов,
кандидат політичних наук,
державний експерт відділу інформаційної безпеки
та міжнародних інформаційних відносин
Національного інституту проблем міжнародної безпеки
РНБО України

Стаття присвячена проблемі формування кібербезпекової політики США за адміністрації президента Барака Обами і практичних кроків, що робилися керівництвом США в цьому напрямі протягом 2008 - 2009 років.

Ключові слова: *інформатизація, весвітня Мережа, кібербезпека, кіберзброя.*

The article is dedicated to the problem of forming the USA cybersecurity policy while the president Barack Obama's administration and practical steps made by the USA leaders in this direction in 2008-2009.

Keywords: *informatization, worldwide net, cybersecurity, cyberweapon.*

Актуальність проблеми

Розвиток інформаційних технологій, інтенсивна інформатизація не лише органів державного управління, але й усієї системи життєзабезпечення суспільства, виводять проблеми забезпечення кібербезпеки на якісно новий рівень, який є практично співставним з військовою безпекою держави.

Поширення новітніх інформаційних технологій в країнах, що розвиваються (в яких контроль держави за злочинністю у цій сфері здійснюється лише частково), та світова фінансова криза стають чинниками швидкого зростання кількості злочинних угруповань, які діють

винятково у всесвітній Мережі. Більше того, можливості Інтернету та включеність мережі до критично важливих для функціонування держави систем породжують розвиток наступальних кібертехнологій та, відповідно, створення нового типу зброї – кіберозброї. Все це обумовлює характер викликів у сфері безпеки, що постали перед адміністрацією президента США Б. Обами.

Метою статті є узагальнення сучасних тенденцій політики адміністрації президента США Б. Обами в сфері кібербезпеки.

Проблеми інформаційної безпеки та кібербезпеки активно вивчають як зарубіжні, так і вітчизняні науковці. Активно досліджуються такі аспекти проблем інформаційної безпеки, як інформаційна безпека у контексті глобалізації і трансформації безпекових викликів (А. Леонов [1; 2], Є. Макаренко [3], М. Ожеван [4]), інформаційні та кібервійни (Р. Шафранскі [5], М. Лібіцкі [6], М. Присяжнюк [7]), проблеми формування політики (в тому числі й правової) протидії комп'ютерній злочинності (В. Бутузов [9], О. Климчук, Д. Мельник [8]).

Сполучені Штати Америки є однією з найбільш інфопотужних країн, яка характеризується надзвичайно високим рівнем проникнення інформаційно-комп'ютерних технологій в життя суспільства. Актуальність кібербезпекової проблеми було усвідомлено керівництвом США ще наприкінці 1980-х років, однак перші системні документи в цій царині з'явились фактично за другої каденції адміністрації Б. Клінтона і двох адміністрацій Дж. Буша-молодшого (зокрема, 2003 року було ухвалено „Національну стратегію захисту кіберпростору" [10]).

До останнього часу в США основне навантаження із захисту кіберпростору було покладено на ФБР, Управління внутрішньої безпеки та Секретну службу (водночас активну підтримку їм надають інші силові відомства і служби). Зокрема, у складі ФБР 1996 року було створено кіберпідрозділ (Cyber Division FBI), який функціонує на правах окремого управління в структурі ФБР. На нього покладено функцію надання допомоги іншим підрозділам ФБР у розслідуванні злочинів, вчинених з використанням комп'ютерних і телекомунікаційних технологій. Секретна служба, що входить до складу Міністерства фінансів США, розслідує переважно фінансові злочини [цит. за 9].

Політика Б. Обами у сфері кібербезпеки є значно активнішою, ніж політика його попередника Дж. Буша-молодшого. Не в останню чергу це пов'язано з особистою позицією нового президента США як активного користувача новітніх інформаційних технологій. Його передвиборча кампанія, на думку багатьох політологів (та і за зізнанням самого Б. Обами і його політтехнологів [11]), була виграна значною мірою завдяки широкому використанню можливостей мережі Інтернет.

Відповідно, нова Адміністрація з самого початку визначила питання

зарубіжний досвід

кібербезпеки в якості одного з ключових у своїй політиці. Віце-президент США Дж. Байден під час церемонії представлення нового керівника ЦРУ Л. Панетта навіть назвав політику нової адміністрації у сфері кібербезпеки „однією з трьох основних" поряд з політикою США в Афганістані та Іраку [12].

Для такої прискіпливої уваги з боку нового керівництва США до проблеми кібербезпеки є дві ключові передумови.

По-перше, курс на збільшення інвестицій в інфраструктурні проекти (до яких можна віднести й комп'ютерну інфраструктуру) дасть можливість забезпечити новими держзамовленнями американську IT-індустрію, котра, як і більшість інших сфер економіки, переживає не найкращі часи після фінансово-економічної кризи 2008 – 2009 років.

По-друге, в США все більше посилюється активність хакерів. За даними сайту America.gov [13], 2006 року лише сайт міністерства оборони піддавався атаці 6 мільйонів разів, а 2008 року кількість таких спроб зросла до 360 мільйонів. На думку генерал-лейтенанта К. Александера, який очолює Агентство національної безпеки США, найбільшу небезпеку для США становлять Росія і Китай, які „активно готують спеціалістів для війни в кіберпросторі".

9 лютого 2009 року, одразу після перших призначень до апарату нової адміністрації, Б. Обама видав розпорядження про підготовку у 60-денний термін „Огляду кібербезпеки" (Cyber Security Review) [14], що мав на меті „виробити стратегічну основу для кіберініціатив уряду США" [15]. В цьому Огляді, презентованому 29 травня 2009 року, до ключових завдань керівництва США у сфері кібербезпеки віднесено:

- забезпечення центральної ролі Білого Дому у формуванні кібербезпекової політики, що має на меті продемонструвати аудиторії як в США, так і на міжнародному рівні серйозність намірів американського керівництва у сфері кібербезпеки;
- перегляд законодавства і політики у сфері кібербезпеки;
- посилення федерального лідерства та відповідальності у сфері кібербезпеки;
- просування лідерських проектів державного, регіонального і локального рівня.

Крім того, в цьому документі окреслено ключові завдання, що мають на меті посилити кібербезпеку США:

- підвищити готовність суспільства до кіберзагроз;
- посилити кібербезпекову освіту;
- збільшити кількість федеральних працівників, що розуміються на інформаційних технологіях;
- просувати кібербезпеку як важливий елемент відповідальності урядів всіх рівнів.

Особливу увагу адміністрація Б.Обами надає проблемі організаційного і кадрового забезпечення реалізації кібербезпекової політики. 5 березня

2009 року було призначено федерального директора з інформаційних технологій, до посадових обов'язків якого входить питання інформаційної безпеки та координації всіх оргструктур, задіяних в системі кібербезпеки держави [16]. 9 лютого 2009 року було запроваджено посаду виконуючого обов'язки керівника кібербезпеки Ради національної та внутрішньої безпеки (яку до серпня 2009 року обіймала М. Хатавей, що одночасно була призначена відповідальною за підготовку „Огляду кібербезпеки"). Одразу зі вступом Б. Обами на посаду президента США було призначено і помічника президента з питань внутрішньої безпеки та контертерроризму (Дж. Бренон), який також безпосередньо опікується питаннями кібербезпеки.

Свої основні погляди на проблему кібербезпеки Б. Обама оприлюднив 29 травня 2009 року у „Зауваженнях щодо забезпечення національної кіберінфраструктури"[18]. Він відзначив, що „цей світ – кіберпростір – це світ, від якого ми залежимо щодня. Кіберпростір реальний, а отже і загрози в ньому цілком реальні". На думку Б. Обами, рівень кіберзлочинності сягнув такого рівня, що поставив під загрозу добробут американців: лише за останні два роки збитки від діяльності кіберзлочинців коштували американцям 8 млрд. доларів. Наводячи приклади кібервтручань терористів у федеральні мережі США (у сфері військової безпеки, енергетики, водопостачання тощо), Б. Обама робить висновок, що „кіберзагрози є одним з найбільш серйозних викликів економічній та національній безпеці, з яким зустрілася нація".

Б. Обама окреслив п'ять основних напрямів, що мають на меті забезпечити вирішення означених проблем: розробка ефективної стратегії забезпечення безпеки інформаційних та комунікаційних мереж; розробка систем запобігання кібератакам; посилення партнерства між державою і приватним сектором; збільшення інвестицій в інновації технології та в інформаційні інфраструктури; початок широкої національної компанії щодо посилення готовності суспільства до кіберзагроз.

Б. Обама повідомив про створення при Білому Домі відділу з кібербезпеки, в обов'язки якого буде входити координація роботи урядових відомств, що опікуються комп'ютерною безпекою, розслідуванням кіберзлочинів і хакерських атак, а також розробкою нових захисних технологій.

В той же день, 29 травня, у газеті The New York Times з'явилось повідомлення про бажання керівництва Пентагону створити спеціальне командування для ведення війн в кіберпросторі [19], а 24 червня 2009 року міністр оборони Р. Гейтс заявив [20], що вже найближчим часом в структурі його відомства буде створено кіберкомандування США (U.S. Cyber Command), яке підпорядковуватиметься безпосередньо Стратегічному командуванню (United States Strategic Command).

Поки такий підрозділ не створено, Б. Обама посилює традиційні безпекові

зарубіжний досвід

інституції, що також опікуються проблемами кібербезпеки. В лютому 2009 року для запобігання можливості „зламу" урядових комп'ютерних мереж були розширені повноваження Агентства національної безпеки США щодо контролю над кіберпростором країни (включно з можливістю втручатись в мережеві підсистеми федеральних та місцевих адміністрацій) [21]. Крім того, для посилення контролю за мережею Інтернет уряд США на 2010 рік виділив ФБР додатково 234 млн. доларів для спеціального проекту з прослуховування Інтернет (Advanced Electronic Surveillance - Going Dark) [22]. В першу чергу цей проект спрямований на можливість прослуховування Інтернет-комунікаторів (наприклад, Skype). З 1 жовтня 2009 року в США оголошено про набір додатково тисячі співробітників до спеціального кібербезпекового департаменту Управління національної безпеки (Department of Homeland Security), які опікуватимуться винятково безпекою високотехнологічних систем [23]. Однак навіть ця кількість співробітників не повністю відповідає потребам США у фахівцях з кібербезпеки. В супровідному документі до спеціально організованих урядом „Кіберзмагань США" (U.S. Cyber Challenge) наводиться думка одного з експертів, що реальна потреба уряду в таких фахівцях складає від 10 до 30 тисяч [24].

Наприкінці квітня 2009 року сенатори О. Сноу і Д. Рокфеллер підготували законопроект [25], який надасть президентові Б. Обамі доступ до „другої червоної кнопки", за допомогою якої він зможе у надзвичайних випадках загроз національній безпеці відмкати доступ до мережі Інтернет по всій території США. Крім того, 9 липня 2009 року сенатор К. Джілібренд запропонував [26] законопроект, згідно з яким США зможуть співпрацювати з будь-яким урядом світу для організації глобальної відсічі нападникам у кіберпросторі (Fostering a Global Response to Cyber Attacks Act). Законопроект запрацює лише у випадку підписання відповідних міжнародних угод, а поки що поширюватиметься лише на співпрацю США з найближчими союзниками, передусім з Великою Британією.

Незважаючи на таку активну внутрішню політику у сфері інформаційної та кібербезпеки, постійні звинувачення на адресу Росії та Китаю у загрозі національній безпеці США починають зустрічати протидію з боку цих країн. Так, представник Міжвідомчої комісії з інформаційної безпеки Ради безпеки РФ В. Шерстка озвучив звинувачення на адресу США щодо їх активного небажання реально співпрацювати у сфері кібербезпеки (зокрема, в межах ООН, та протидії прийняття на міжнародному рівні універсального міжнародно-правового документа, що має констатувати наявність загроз міжнародній інформаційній безпеці та передбачав би можливість здійснення спільних дій з мінімізації негативних наслідків національним інтересам окремих країн та інтересам міжнародної спільноти в цілому[27].

Висновки

Активна кампанія посилення кібербезпеки США за нового президента свідчить про поступову зміну „жорсткого підходу", характерного для адміністрації Дж. Буша-молодшого, політикою „м'якої безпеки", яка в працях її ідеолога Дж. Ная пов'язується з поняттям „інфолідерства".

Незважаючи на проголошену політику забезпечення, передусім, безпеки кіберпростору, за своїм характером політика Б. Обами більше нагадує створення нового фронту глобальних „перегонів озброєнь", що може лише посилити рівень напруги між ключовими гравцями кіберпростору. Декларована новою адміністрацією політика „убезпечення" вже в найближчому майбутньому може еволюціонувати в дискурси „тотальної безпеки" і призвести до створення нових концепцій кібервоєн.

Водночас слід зазначити, що така увага до створення, передусім, кібервійськ та готовності до ведення кібервоєн, змушує США включитись у парадоксальний, з огляду на проголошені завдання з забезпечення саме безпеки кіберпростору, процес, з одного боку збільшення інформатизації регіонів, що розвиваються, оскільки ефективна інформаційна протидія (агресії) можлива лише в умовах еквівалентності розвитку потенційного противника, тобто збільшення проникнення інформаційних технологій в систему державного управління, як це відбувається в США, а з іншого – подальше збільшення рівня інформатизації власне США, що безумовно призводитиме до збільшення можливостей заподіяння шкоди інформаційній інфраструктурі.

Перспективи подальших розвідок

Вбачаються перспективними подальші дослідження формування кібербезпекової політики провідних держав світу (Велика Британія, Німеччина, Франція, Японія, Китай, Росія) і того впливу на міжнародне політичне поле, яке може спричинити подальша мілітаризація кіберпростору.

Література:

1. Леонов А. П. Актуальные проблемы информационной безопасности в контексте глобализации [Электронный ресурс] / А. П. Леонов. – Режим доступа: www.itsec.ru/doc/leonov.doc.

2. Леонов А. П. О предпосылках формирования новой парадигмы информационной безопасности для первого десятилетия XXI в. / А. П. Леонов // Компьютерная преступность и информационная безопасность / Под общ. ред. А. П. Леонова. – М.: АРИЛ, 2000. – С. 9 - 81.

3. Макаренко Є. А. Міжнародна інформаційна безпека у глобальній системі підтримання миру і стабільності (концептуальний вимір) // Міжнародна інформаційна безпека: сучасні виклики та загрози / [Макаренко Є. А., Гондюл В. П., Рижков М. М. та ін.]. – К.: Центр вільної

зарубіжний досвід

преси, 2006. – С. 9 - 28.

4. Ожеван М. А. Україна у структурі європейської інформаційної безпеки / М. А. Ожеван // Європейські комунікації: політичні, економічні, правові, безпекові, дипломатичні, суспільні та культурні аспекти: [кол. монографія] / [Макаренко Є. А., Гондюл В. П., Рижков М. М. та ін.]. – К. : Центр вільної преси, 2007. – С. 247 - 260.

5. Szafranski R. A Theory of Information Warfare [Electronic resource] / R. Szafranski. – Access mode: http://www.iwar.org.uk/iwar/resources/airchronicles/ szfran.htm.

6. Libicki M. C. Cyberdeterrence and Cyberwar / M. C. Libicki. – Pub. by RAND, 2009. – 238 p.

7. Присяжнюк М. М. Інформаційна зброя як засіб ведення інформаційної боротьби держави / М. М. Присяжнюк // Інформаційна безпека: людини, суспільства. - 2009. - №1. - С. 20 - 29.

8. Климчук О. О., Мельник Д. С. Реалізація положень про кіберзлочинність в законодавстві України / О. О. Климчук, Д. С. Мельник // Інформаційна безпека: людини, суспільства, держави. - 2009. - №1. - С. 39 - 43.

9. Бутузов В. М. Протидія комп'ютерній злочинності: деякі аспекти міжнародного досвіду (на прикладі діяльності правоохоронних органів США та Німеччини) / В. М. Бутузов // Інформаційна безпека: людини, суспільства, держави. - 2009. - №1. - С. 30 – 38.

10. National Cyberspace Strategy [Electronic resource] / Department of Homeland Security. – Access mode: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

11. В Минске раскрыли секреты избирательной кампании Барака Обамы [Электронный ресурс] / Interfax.by. – Режим доступу: http://www.interfax.by/article/40963

12. Remarks by the Vice President at the ceremonial swearing-in of Leon E. Panetta as director of the CIA [Electronic resource] / White House. – Access mode: http://www.whitehouse.gov/the_press_office/Remarks-by-the-Vice-President-at-the-ceremonial-swearing-in-of-Leon-E-Panetta-as-D/

13. Страны защищают компьютерные сети и веб-сайты [Электронный ресурс] / БМИП Государственного департамента США. – Режим доступу: http://www.america.gov/st/peacesec-russian/2009/October/20091002140506sjhtrop0.8408167.html

14. Cyberspace Policy Review [Electronic resource] / White House. – Access mode: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

15. President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review [Electronic resource] / White House. – Access mode: http://www.whitehouse.gov/the_press_office/advisorstoconductimmediatecybersecurityreview/

16. President Obama Names Vivek Kundra Chief Information Officer [Electronic resource] / White House. – Access mode: http://www.whitehouse.

gov/the_press_office/President-Obama-Names-Vivek-Kundra-Chief-Information-Officer/

17. Statement by the President on the White House Organization for Homeland Security and Counterterrorism [Electronic resource] / White House. – Access mode: http://www.whitehouse.gov/the_press_office/Statement-by-the-President-on-the-White-House-Organization-for-Homeland-Security-and-Counterterrorism/

18. Remarks by the President on securing our nation's cyber infrastructure [Electronic resource] / B.Obama. – Access mode: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

19. Sanger D., Shanker T. Pentagon plans new arm to wage cyberspace wars [Electronic resource] / D.Sanger, T.Shanker. – Access mode: http://www.nytimes.com/2009/05/29/us/politics/29cyber.html?_r=1

20. Gates Establishes New Cyber Subcommand [Electronic resource] / D.Miles. – Access mode: http://www.defenselink.mil//news/newsarticle.aspx?id=54890

21. АНБ США получит право регулировать киберпространство США [Электронный ресурс] / Cybersecurity.ru. – Режим доступу: http://www.cybersecurity.ru/armament/65241.html

22. ФБР получит $ 234 миллиона на новые средства слежки за Интернетом [Электронный ресурс] / Newsru.com. – Режим доступу: http://hitech.newsru.com/article/15jun2009/fbi

23. DHS Seeking 1,000 Cyber Security Experts [Electronic resource] / B. Krebs. – Access mode: http://voices.washingtonpost.com/securityfix/2009/10/dhs_seeking_1000_cyber_securit.html

24. The United States Cyber Challenge [Electronic resource] / White House. – Access mode: http://www.whitehouse.gov/files/documents/cyber/The%20United%20States%20Cyber%20Challenge%201.1%20%28updated%205-8-09%29.pdf

25. The Cybersecurity Act of 2009 [Electronic resource] / O.Snowe. – Access mode: http://www.snowe.senate.gov/public/index.cfm?FuseAction=PressRoom.PressReleases&ContentRecord_id=8D76A8BB-802A-23AD-4384-78D04C8509A9

26. Fostering a Global Response to Cyber Attacks Act (Introduced in Senate) [Electronic resource] / K.Gillibrand. – Access mode: http://thomas.loc.gov/cgi-bin/query/z?c111:S.1438:

27. Россия - Болгария: информационное сотрудничество и информационная безопасность [Электронный ресурс] / Н. Димлевич. – Режим доступу: http://www.fondsk.ru/article.php?id=2506