УДК 351/354

Т. В. Запорожець
кандидат наук з державного управління,
доцент кафедри глобалістики, євроінтеграції
та управління національною безпекою
Національної академії державного управління при Президентові України

БЕЗПЕКА ІНФОРМАЦІЙНОГО ПРОСТОРУ В УМОВАХ ГЛОБАЛІЗАЦІЇ

Стаття присвячена дослідженню проблеми забезпечення безпеки інформаційного простору в сучасних умовах глобалізації та виробленню на цій основі пропозицій щодо підвищення ефективності вітчизняної державної політики в досліджуваній сфері у тому числі щодо сприяння подолання так званого «цифрового розриву».

Ключові слова: *державна політика, безпека інформаційного простору, державне регулювання, ефективність державної політики.*

Постановка проблеми. На сучасному етапі переходу світового співтовариства до інформаційного суспільства ступінь розвитку інформаційного простору та інформаційних технологій стає безпосереднім чинником становлення активного та свідомого громадянина, національної конкурентоспроможності. Зазначений етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення й використання інформації, а також системи регулювання відносин, що виникають при цьому.

Забезпечення безпеки інформаційного простору є одним із найбільш важливих чинників стимулювання економічного зростання та розвитку громадянського суспільства, зайнятості населення, розширення конкуренції і, як наслідок, сприяння подоланню так званого «цифрового розриву».

Аналіз останніх досліджень і публікацій. Науковому осмисленню феномена інформатизації й вивченню змісту процесу формування інформаційного суспільства присвячені роботи зарубіжних теоретиків: Д. Белла, Е. Тоффлера, Т. Стоуньєра, А. Турена, У. Дайзарда, М. Кастельса, К. Кояма, Й. Масуди; українських дослідників: В. Литвиненка, Е. Макаренка, О. Сосніна, Л. Шиманського, С. Янишевського й інших.

Правові й державно-управлінські основи захисту інформації розкриваються в дослідженнях українських учених Б. Авер'янова, О. Баранова, О. Копиленка, Б. Кормича, Р. Марутян, В. Погорілка, Г. Почепцова тощо.

Мета статті – здійснити детальний аналіз проблеми забезпечення безпеки інформаційного простору в сучасних умовах глобалізації та вироблення на цій основі пропозицій щодо підвищення ефективності вітчизняної державної політики в досліджуваній сфері, в тому числі щодо сприянню подолання так званого «цифрового розриву».

Виклад основного матеріалу. Стрімке зростання комп'ютеризації основних сфер людської діяльності, що охоплює управління державою, збройними силами, роботою ядерних реакторів, хімічних заводів, фінансово-банківську діяльність, вивчення космосу й подібне, з одного боку, дозволило забезпечити високі досягнення в галузі науки, техніки, культури, управління й організації життєдіяльності суспільства в цілому. З іншого боку, наявність глобальних комп'ютерних мереж і недостатня їхня захищеність від збоїв техніки, викликаних всілякими причинами, від неправомірних дій людей, здійснених навмисно або з необережності, можуть викликати найбільш непередбачені, шкідливі для людини й суспільства наслідки.

Віру громадян у швидкий наступ інформаційного суспільства підривають і дії комп'ютерних зловмисників, здатних порушувати нормальну роботу стратегічно важливих державних об'єктів. Можна згадати випадок, коли злочин-

на група спробувала розбалансувати систему управління польотами Франкфуртського міжнародного аеропорту. Зловмисники, які володіли необхідними спеціальними знаннями, паралізували роботу систем попередження й вивели з ладу кабельні лінії, по яких забезпечувався комп'ютерний, факсимільний й телефонний зв'язок між трьома рознесеними у просторі станціями спостереження [1].

Перший у ФРН напад комп'ютерних терористів не привів, на щастя, до серйозних наслідків: графік руху повітряних суден порушився лише на дуже незначний інтервал часу, а системи управління й комунікації були швидко відновлені. Але вже через два місяці після цього інциденту ланцюг збоїв в електронній системі Бундесбана (Управління залізниць у Німеччині) вивів з рівноваги десятки тисяч пасажирів, подорож яких на ділянці дороги «Гамбург-Алтона» раптово призупинилася. Причиною події виявився невідрегульований комп'ютер у системі управління [2, с. 384].

Як зазначав Г. Бехманн, «Інтернет – своєрідна сполучна тканина або павутина нашого життя. Це не майбутнє – це сьогодення. Інтернет став медіумом для всього, що вступає у взаємодію із суспільством як цілісністю. І хоча у своїх соціально релевантних формах він ще дуже молодий (Інтернет виник між 1969 і 1994 р. у міру розвитку браузера World Wide Web), уже не потрібно занадто довго пояснювати, що це таке» [3, с. 23].

Вже стало очевидним, що поширення Інтернет-технологій у політику розширює можливості політичної участі населення і є кроком до громадянського суспільства.

Разом із тим простір Інтернет породжує й нові злочини. Поява електронних мереж створила якісно нові умови й для пропаганди терористами своїх ідей, для ведення ними відкритої полеміки з офіційними державними структурами, дискредитації й дезавуювання заяв офіційної влади. Не слід забувати й ту обставину, що з комп'ютеризацією адміністративно-управлінських процесів терористи одержали можливість використовувати у своїх цілях відносно дешеві й доступні методи інформаційно-комп'ютерних диверсій. Поки під удар потрапляють найбільш розвинені країни, в яких широко поширені відкриті електронні системи. Насамперед, це відноситься до США й Канади.

Науково-технічний прогрес розширює можливості міжнародного тероризму до провокування ядерних, екологічних, інформаційних та інших глобальних катастроф. Тому винятково більшу небезпеку в сучасних умовах представляє технологічний тероризм, що включає в себе інформаційний тероризм (кібертероризм, біотероризм, «ядерний тероризм») і можливе використання ядерних матеріалів, що розщеплюються, і хімічної зброї.

Політична мета кібертероризму – нагнітання суспільної напруженості, страху, дестабілізація обстановки, дискредитація офіційної влади. Фактичною метою його атак виступають комп'ютерні системи управління критичною інфраструктурою, тобто транспортом, атомними електростанціями, водопостачанням і енергетикою [4].

Інтернет-технології надають екстремістам унікальну можливість ведення інформаційної війни з державою методом безпосереднього й безконтрольного поширення своїх ідей, гасел, закликів у вигляді звертань до широкої аудиторії через сайти, форуми й чати, файлообмінні мережі.

Головна небезпека полягає в тому, що до Інтернету підключена в основному молодь, тобто соціальна група, найбільш сприйнятлива до екстремізму. Екстремістські інформаційні ресурси в Інтернеті при грамотному їхньому розміщенні оперативно придушити досить складно, тому що треба зв'язатися із представниками влади тої країни, де розташований сервер,що обслуговує екстремістів, виконати всі відповідні юридичні формальності – все це вимагає часу й фінансових витрат. Навіть швидке ознайомлення з каталогом ресурсів радикалів в українській мережі показує, що багато які із сайтів розташовані за межами зони UA. У цьому зв'язку зростає роль служб, відповідальних за безпеку держави й протидію кібертероризму [5].

Отже, в ході глобальної інформатизації виникло принципово нове середовище протиборства конкуруючих держав – кіберпростір. Якщо у світі до теперішнього часу склався в тому або іншому ступені стратегічний баланс сил у галузі звичайних озброєнь і зброї масового знищення, то питання про паритет у кіберпросторі залишається відкритим.

У процесі формування кіберпростору відбувається конвергенція військових і цивільних комп'ютерних систем і технологій. Державні органи все ширше закуповують для вирішення військових та інших спеціальних завдань апаратно-програмні засоби, розроблені комерційними виробниками для широкого кола користувачів.

Росте також потреба в сумісності громадянської інформаційної інфраструктури з урядовою й військовою. У зв'язку із цим відбувається їх

технологічне й організаційне злиття. Так, 95% ліній зв'язку комп'ютерних мереж Міністерства оборони США розгорнуто на базі загальнодоступних телефонних каналів, а понад 150 тис. комп'ютерів підключені до мережі Інтернет, що робить їх надзвичайно вразливими [6].

Весь стандартизований комп'ютерний комплекс може бути швидко виведений із ладу застосуванням одного конкретного засобу, атакою, орієнтованою на загальний для стандартизованої мережі вразливий елемент, наприклад операційну систему або протокол зв'язку.

Зазначена обставина може бути ефективно використана радіоелектронною розвідкою країни-розроблювача цих уніфікованих платформ.

Лідируюче положення в цій сфері займають США, що розглядають світову інформаційну інфраструктуру як сферу, контроль над якою дозволить здійснити стратегічні цілі глобального домінування. У формуванні їхньої зовнішньої політики з'явився новий підхід, пов'язаний із поняттям «інформаційної парасольки», коли США беруть на себе забезпечення інформаційної безпеки своїх союзників [7].

Ця позиція зустрічає протидію з боку розвинених країн. Наприклад, Японія вважає, що введення інформаційної парасольки може привести до втрати суверенітету країни.

Американська адміністрація вважає, що формування єдиної глобальної інформаційної інфраструктури під контролем США дозволить їм вирішити завдання стратегічного використання інформаційної зброї «аж до блокування телекомунікаційних мереж держав, що не визнає реалії сучасної міжнародної системи».

На думку західних аналітиків, ЦРУ й військова розвідка США вивчають можливості й методи проникнення в комп'ютерні мережі своїх потенційних супротивників. Для цього, зокрема, розробляються технології впровадження електронних вірусів і «логічних бомб», які, не проявляючи себе у звичайний час, здатні активізуватися по команді [8, с. 86].

У кризовій ситуації «електронні диверсанти» можуть дезорганізувати оборонну систему управління, транспорт, енергетику, фінансову систему іншої держави. Перспективними для таких цілей уважаються «заражені» мікросхеми, що впроваджені в експортовану Сполученими Штатами обчислювальну техніку.

Так, у Пентагоні активно дискутуються питання створення й використання електронних і комп'ютерних засобів атаки на військову техніку й об'єкти військової інфраструктури ймовірного супротивника.

Причому справа не обмежується теоретичною дискусією. Один із головних ентузіастів кіберзброї в Пентагоні М. Уінн створив в 2007 році кіберкомандування для проведення операцій у кіберпросторі, включаючи в тому числі й наступальні (перехоплення контролю над безпілотними літальними апаратами супротивника, виведення з ладу ворожих літаків у польоті, супровід авіаударів електронною атакою на системи ПВО й т.д.).

Крім того, Міністерство оборони США активізувало розробку підходів до ведення бойових дій у кібернетичному просторі.

Основною метою зусиль, що вживаються, є формування вигляду майбутніх сил ведення бойових дій у кіберпросторі й визначення їхніх бойових можливостей на тлі прискореного розвитку технологій мережних комп'ютерних операцій, радіоелектронної боротьби, радіоелектронної розвідки, а також зброї спрямованої енергії. І все це – для контролю над кіберпростором, що обіцяє в недалекому майбутньому військову перевагу США над супротивниками [9].

Якщо раніше вектор державної політики в галузі забезпечення інформаційної безпеки був більш орієнтований на загрозу (в кіберпросторі можуть представляти терористичні й кримінальні угрупування – спецслужби очікували інспірованих катастроф літаків і поїздів, техногенних аварій), то тепер акценти у сфері міжнародної безпеки змістилися убік повномасштабної системи захисту інформації.

Поява нових загроз породила політичну необхідність контролю (регулювання) кіберпростору, прийняття відповідних норм. Пріоритетність питань кібербезпеки для подальшого розвитку Інтернету визнана найвищою на Всесвітньому саміті з інформаційного суспільства. Причому управління інформаційним простором необхідне не тільки для забезпечення національної безпеки абсолютного ІТ-Лідера – США, але й міжнародної безпеки в цілому.

Висновок. Викладене дозволяє зробити висновок про те, що в українських умовах істотну небезпеку стабільності політичної системи несе Інтернет. Це зв'язано головним чином із відсутністю ефективних правових механізмів, що регулюють життя в Інтернет-просторі. У результаті система інформаційно-політичних відносин трансформується не просто в поле інформаційного протиборства, а війну компроматів, де не

останнє місце займає «чорний піар». Поряд з офіційними сайтами органів державної влади, політичних партій, громадських організацій в Інтернеті створюються інформаційні майданчики для «вкидання» в суспільство компромату на ту або іншу політичну силу, тому що практично ніяких обмежень на характер інформації, що вноситься в Мережу, не існує.

Більше того, сучасні Інтернет-Технології сприяють розростанню міжнародного тероризму й виникненню принципово нового високотехнологічного кібертероризму. При цьому можуть застосовуватися як інформаційно-комп'ютерні, так і інформаційно-психологічні засоби. Інтернет же все активніше використовується для поширення ідеології тероризму, залучення в протиправну діяльність нових членів, про що красномовно свідчить наявність великої кількості відповідних сайтів.

Усі ці обставини свідчать про гостру потребу держави постійно зміцнювати інформаційну безпеку, сприяти усуненню загроз, пов'язаних із використанням інформаційно-комп'ютерних технологій.

Нейтралізувати вплив інформаційних загроз покликана єдина державна система інформаційної безпеки України як організаційне об'єднання державних органів, сил і засобів інформаційної безпеки. У завдання цієї системи входить: виявлення й прогнозування появи дестабілізуючих факторів і інформаційних загроз життєво важливим інтересам особистості, суспільства й держави; здійснення комплексу довгострокових і оперативних заходів для їхнього попередження й усунення; створення й підтримка в готовності сил і засобів забезпечення інформаційної безпеки.

Список використаної літератури:

1. Гавловський В. Інформаційна безпека: заГавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект). URL: www. bezpeka. com/ru/lib/spec/law.html.
2. Недбай В.В. Інтернет-комунікації – нові можливості та нові проблеми // Політологічний вісник. Зб-к наук. праць. К.: «ІНТАС», 2009. Вип. 39. С. 379.
3. Бехманн Г. Современное общество. Общество риска, информационное общество, общество знаний. М.: Логос, 2010. 248 с.
4. Галамба М. Інформаційна безпека України: поняття, сутність та загрози. URL: http://www.nbu.gov.ua/infan/arxiv/arxiv0/2007/01/28.
5. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.
6. Дрожжина В., Штрик А. IT як приводний ремінь підвищення ефективності державного управління в США. URL: http://www.pcweek.ru/.
7. Леваков А. В США готовятся к защите информационных систем. URL: http://ww–4.narod.ru/index.html.
8. Фріден Р. М., Дрейк В. Дж. Глобальна інформаційна інфраструктура / Телекомунікації в умовах інформаційної доби / Інформаційна Агенція Сполучених Штатів. 2000 С. 85.
9. ВВС США усиливают подразделения для проведения кибероперацій гражданскими лицами // IT Expert (http://itexpert.org.ua/rubrikator/item/21915-vvs-ssha-usilivaiut-podrazdeleniyadlya-provedeniya-kiberoperatsiy-grazhdanskimi-litsami.html).

Запорожец Т. В. Безопасность информационного пространства в условиях глобализации

Статья посвящена исследованию проблемы обеспечения безопасности информационного пространства в современных условиях глобализации и выработке на этой основе предложений по повышению эффективности отечественной государственной политики в исследуемой сфере и содействию преодоления «цифрового разрыва».

Ключевые слова: *государственная политика, безопасность информационного пространства, государственное регулирование, эффективность государственной политики.*

Zaporozhets T. V. Security of information space in the conditions of globalization

The article is devoted to the study of the problem of ensuring the security of the information space in the current conditions of globalization and elaborating on this basis proposals for improving the efficiency of domestic state policy in the investigated sphere and helping to overcome the «digital divide».

Key words: *state policy, information space security, state regulation, efficiency of state policy.*