Щепанківський В.Г.*

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА СУЧАСНОГО ОБРАЗУ КРАЇНИ

В этой статье рассматривается понятие информационной безопасности как составляющей образа страны. Анализируются понятие информационная безопасность ее основные аспекты и характеристики ее важности для мирового сообщества и разных стран в отдельности.

Ключевые слова: информация, безопасность, образ, страна, угроза.

В даній статті розглядається поняття інформаційної безпеки як складової образу держави. Аналізується поняття інформаційної безпеки її основні аспекти і характеристики та її важливість для міжнародної спільноти і різних країн окремо.

Ключові слова: інформація, безпека, образ, країна, загроза.

In this article the concept of information security as is considered by a component an image of the country. Its basic aspects and characteristics its importance for the world community and the different countries separately are analyzed concept information security.

Keywords: information, security, image, country, threat.

Швидка експансія новітніх інформаційних технологій, різноманітних видів мультимедіа та засобів глобальної комунікації призвела до виникнення принципово нових видів людської діяльності, заснованих на поняттях та образах віртуального простору. Нова інформаційна економіка, коммунікативістика, філософія мас–медіа або імагологія, віртуальна географія, крос–культурні дослідження, країнознавча компаративістика та інформаційна геополітика змушені оперувати так званими «анаморфірованими географічними просторами». Ці простори схожі за певними параметрами з традиційним географічним простором, проте закони їх створення, функціонування та трансформації є певною мірою автономними, оскільки ці простори представляють собою самостійний предмет гуманітарно–наукового вивчення, що пов'язане з жорсткою спеціалізацією їх конфігурацій і змісту. Отже, мова йде про конкретні геоекономічні, геополітичні та геокультурні простори.

В епоху бурхливого розвитку віртуальних та мультимедійних уявлень, що швидко проникають до науки, образна складова будь–якого знання перетворилася на важливий фактор досліджень. Постмодерн пропонує замість єдиного образу світу «віяло» (рос. «веер») або карточну колоду географічних образів, кожний з яких створює самостійну просторову версію світу, яка не заперечує інших. Парадокс образної геоглобалістики або

* аспірант кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка
Науковий керівник: проф. Рижков М.М.

створеної російським культурологом і географом Д. Замятіним гуманітарної географії полягає в неможливості достатньо коректного формування єдиного географічного образу світового розвитку [1]. Світовий розвиток – це своєрідна нескінченна мережа образів країн, що створюють множину геополітичних дискурсів.

У сучасному суспільстві інформація та інфосфера є інструментом перетворення географічного простору в геополітичний. Інформаційний ресурс активно впливає на географічний простір, імідж держави, наприклад, визначає розвиток соціально–географічної системи країни. Більшість країн мають геопросторові образи, закріплені в суспільній свідомості у вигляді вербалізованих стереотипів, але держава може формувати і власні геополітичні образи, смисли або контексти. Геополітичний образ можна визначити як політичний метаобраз, що ефективно використовує структурні знання та образи, які мають просторовий вимір.

Фінансові й інформаційні потоки, літературні та художні твори, локальні культурні співтовариства, політичне та інформаційно–психологічне протиборство створюють «приватизовані географоїдні простори», які можна репрезентувати та інтерпретувати як специфічні геоекономічні, геокультурні та віртуальні образи.

Головним складовим елементом образу країни у сучасному світі можна визначити багатостороннє поняття як інформація. Аналізуючи зміст та роль інформації у сучасному світі, американський дослідник Маршалл Маклюен виводить цікаву тезу: «Істинно тотальна війна – це війна за допомогою інформації» [2]. Саме він першим проголосив, що в наш час економічні зв'язки і відносини усе більше набирають форму обміну знаннями, а не обміну товарами. А засоби масової комунікації самі є новими «природними ресурсами», що збільшують багатства суспільства. Тобто боротьба за капітал, простори збуту та ін. відходять на другий план, а головним зараз стає доступ до інформаційних ресурсів, знань, що призводить до того, що війни ведуться вже більше в інформаційному просторі та за допомогою інформаційних видів озброєнь. Глобалізація інформаційних ресурсів стає визначальним фактором існування та виживання сучасної цивілізації.

Мета дослідження полягає у з'ясуванні місця поняття міжнародної безпеки як складової образа країни. Досягнення мети дослідження обумовило необхідність розглянути теоретичні підходи та емпіричні дані, що сприяють вирішенню наступних завдань:

1. дослідити нові підходи до розуміння образу країни;
2. визначити основні характеристики і функції поняття «інформаційної безпеки»;
3. на підставі теоретичних та емпіричних розробок, зробити висновки, що до можливості інформаційної безпеки виступати окремою складовою образу країни.

Проблеми глобальної безпеки посідають особливе місце в структурі образу країни, визначають суперечності сучасного етапу міжнародного розвитку, які досягли такого рівня і гостроти, що можуть поставити під загрозу забезпечення світового порядку, реалізацію стратегій становлення глобального інформаційного (інтелектуального) суспільства, навіть саме існування цивілізації. Глобальна безпека як чинник міжнародних відносин, вплив якого має універсальний характер і врахування якого в діяльності міжнародного співтовариства та в зовнішній політиці окремих держав призводить до радикальних змін у поведінці акторів міжнародних відносин, до трансформації самої сутності проблеми безпеки після закінчення «холодної війни» і розпаду біполярної міжнародної системи, потребує концептуального перегляду принципів функціонування міжнародних та національних інститутів, що відповідають за безпеку, а також врахування в нових доктринах інформаційної складової міжнародної безпеки [2, с.9].

Міжнародну безпеку слід розглядати як геополітичну складову, що сприяє створенню ефективних гарантій миру як для окремої країни, так і для всього світового співтовариства.

З–поміж теоретичних поглядів на міжнародну безпеку варто згадати французького теоретика Реймона Арона, який вважав, що безпека у світі незалежних держав може ґрунтуватися або на слабкості суперників (їх повному або частковому роззброєнні), або на власній силі [10].

Зважаючи на глобальність проблеми інформаційної безпеки, розвинуті країни розпочали реалізацію довгострокових державних програм, спрямованих на забезпечення захисту критично важливих інформаційних структур, а з 1996 р. проблему міжнародної інформаційної безпеки було винесено на політичний та міжнародно–правовий рівень:

а) концепцію міжнародної інформаційної безпеки було обговорено на міжнародній конференції з проблем становлення інформаційного суспільства та глобальної цивілізації (ПАР, 1996 р.);

б) у спільному комюніке зустрічі на найвищому рівні США – Російська Федерація було підкреслено загрозу створення інформаційної зброї і визнано наявність воєнної складової глобального процесу інформатизації;

в) на 53–ій сесії ГА ООН було консенсусом прийнято Резолюцію 53/70 від 4 грудня 1998 р., де зазначалося, що міжнародна спільнота визнає проблему інформаційної безпеки як багатоаспектний стратегічний напрям взаємодії держав у світі, пропонувалося державам–членам ООН розглянути конкретну типологію інформаційних загроз, визначити критерії проблеми, включаючи розробку міжнародних принципів безпеки глобальних інформаційних систем, внести пропозиції до комплексної доповіді Генерального секретаря ООН для створення міжнародного механізму протидії використанню інформаційних озброєнь та розпалюванню інформаційних війн [2, с.13–14].

Під час дискусій та розгляду прикладних аспектів міжнародної інформаційної безпеки було визначено специфіку, істотні характеристики та типологію інформаційних загроз, узгоджено термінологію та зміст основних понять в новій сфері міжнародного співробітництва.

Міжнародна інформаційна безпека визначається як взаємодія акторів міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільноти від реальних і потенційних інформаційних загроз.

Інфосфера – міжнародний інформаційний простір, що охоплює інформаційні потоки, інформаційні ресурси та всі сфери життєдіяльності цивілізації. Інфосферу також можна визначити як кіберпростір разом із засобами масової інформації [3].

Міжнародні інформаційні операції характеризуються як форма міждержавного протиборства, яка реалізується з використанням інформаційного впливу на системи управління різного призначення інших держав, а також на політичну владу і суспільство в цілому, на інфраструктуру і ЗМК для досягнення переваги і кінцевої мети інформаційної операції з одночасним захистом національної інфосфери від аналогічних дій.

Інформаційна зброя – комплекс технічних та інших заходів, методів і технологій, спрямованих на встановлення контролю над інформаційними структурами потенційного противника, втручання у роботу його систем управління, інформаційних мереж та комунікацій з метою знищення або модифікації даних, дезінформації, поширення інформації спеціального призначення у системах формування громадської думки і прийняття рішень, а також як сукупність засобів впливу на свідомість і психологічний стан політичних і військових структур, спецслужб та населення для протидії можливим інформаційним впливам іншої сторони [2, с.14–15].

Поняття інформаційної безпеки залежно від його використання розглядається у декількох ракурсах. У найзагальнішому вигляді – інформаційна безпека – це стан захище-

ності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [4, с.38].

Визнання проблеми інформаційної безпеки на міжнародному рівні обумовлюється такими чинниками глобалізації комунікації, як: у більшості індустріально розвинутих країн проводяться дослідження і розробки нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного противника, а за необхідності прямо впливати на них. За даними аналітичних центрів США , розробки такої зброї ведуться в 120 країнах світу: для порівняння розробки в галузі ядерної зброї проводяться у 20 країнах; в деяких країнах завершено розробку засобів інформаційного протиборства (війни) з можливим противником як в умовах воєнних конфліктів різної інтенсивності, так і в мирний час на стратегічному, оперативному, тактичному рівнях та в польових умовах з метою захисту національної інфосфери від агресії і несанкціонованого втручання; в розвинутих країнах концепція інформаційної війни є складовою воєнної доктрини, що обумовлює спеціальну підготовку особового складу і окремих підрозділів для проведення інформаційних операцій; практика міжнародних, регіональних та етнічних конфліктів виявила унікальність застосування інформаційної зброї для впливу на міжнародне співтовариство та для боротьби за геополітичні інтереси [2, с.15].

Багато країн давно займаються політикою захисту інформаційних потоків та систем – не тільки як джерел державних секретів, але і як джерел економічного прибутку. Франція, наприклад, відзначилася у створенні власного сегменту Інтернету на французькій мові. Вона взяла під свій контроль прибутковий ринок комп'ютерної техніки, програмного забезпечення та інформаційних потоків на всьому франкомовному просторі. Відомий досвід Китаю, який досяг суттєвого економічного росту за рахунок переорієнтації інформаційних потоків та акумуляції капіталів в інформаційній сфері [5].

Слід підкреслити, що стратегії глобального інформаційного протиборства лежать в основі аналітичних розробок дослідницьких інституцій різних країн, метою яких є саме забезпечення інформаційного лідерства у сфері міжнародної безпеки. За результатами досліджень аналітики виділяють такі моделі системи глобальної інформаційної безпеки:

– Модель А – створення абсолютної системи захисту країни–інформаційного лідера проти будь–якого виду наступальної інформаційної зброї, що обумовлює об'єктивні переваги в потенційній інформаційній війні, змушує інші країни шукати альянсу у військово–інформаційних діях з країною–інфолідером. При цьому може бути використано систему жорсткого контролю над інформаційним озброєнням противника на підставі потенційних міжнародних документів з інформаційної безпеки.

Погляд на такий розвиток подій покладено у відомому дослідженні Дж. Ная та У. Оуенса «America's Information edge strategy and force planning», 1996 р. («Головна сила Америки – її інформаційні можливості») [6], в якому стверджується домінуюча роль США в інформаційній революції, тобто у використанні надважливих засобів комунікації та інформаційних технологій (супутникового спостереження, прямого мовлення, швидкісних комп'ютерів, унікальних можливостей в інтегруванні складних інформаційних систем), у політиці стримування і нейтралізації традиційних воєнних загроз та нових видів озброєнь.

У сучасному світі, де трансформовано поняття «ядерної парасольки» та стратегії неядерного стримування, наявність інформаційних переваг обумовлює інтелектуальний зв'язок між зовнішньою політикою США та їх військовим потенціалом, збереження світового лідерства за допомогою нових засобів впливу та закріплення домінуючої ролі в альянсах і тимчасових коаліціях. Інформаційне лідерство посилює ефект американської

дипломатії як інструменту «м'якої сили», уможливлює використання інформаційних ресурсів для конструктивного діалогу із потенційними противниками – Китаєм, Індією, Росією та іншими інформаційно–розвинутими країнами з проблем міжнародної безпеки, і одночасно інфолідерство США забезпечує протидію нарощуванню інформаційних озброєнь в потенційно агресивних країнах (Ірак, Пакистан).

Концепція глобальної інформаційної безпеки з точки зору політичних інтересів США полягає у впровадженні доктрини «інформаційної парасольки», що замінить доктрину «ядерної парасольки», на основі взаємовигідного обміну інформацією різного характеру для міжнародної співпраці та підтримки миру.

Проведені в 1999 р. Пентагоном навчання з імітації несанкціонованого проникнення в інформаційні системи воєнного призначення показали, що 88% інформаційних атак увінчались успіхом, із яких 4% були виявлені. За даними американської розвідки сьогодні в 30 країнах світу ведуться програми по створенню засобів інформаційного протиборства (інформаційної зброї), які у майбутньому можуть бути використані проти США [7].

В умовах сучасної інформаційної революції переваги «м'якої сили» США можуть бути використані для остаточного становлення демократичної системи в інших країнах світу, для попередження регіональних конфліктів, для протидії новим загрозам глобального масштабу.

– Модель В – створення значної переваги держави–потенційного ініціатора інформаційної війни в наступальних видах озброєнь, у знешкодженні систем захисту держави–противника засобами інформаційного впливу, координація дій із союзними державами з використаннями визначених засобів інформаційної зброї для ідентифікації джерел і типів інформаційних загроз.

Практичне втілення моделі спостерігається в перебігу інформаційної операції «Союзницька сила» (1999 р.), яку США та країни–члени НАТО здійснили проти Союзної Республіки Югославії. Експерти підкреслюють формування безпрецедентної за масштабами системи управління інформаційними потоками для проведення військових операцій (спроможність надавати розвідувальну інформацію безпосередньо кожному з учасників бойових дій), масових пропагандистських кампаній з широким спектром інформаційних методик (від технологій PR для формування сприятливої світової громадської думки, вибіркового інформування із заданим ефектом сприйняття контенту до всебічної дискредитації політики противника, і навіть відвертої дезінформації світової громадськості), спрямованого інформаційно–психологічного впливу, потужного використання Internet та комп'ютерного протиборства для модифікації національного інформаційного простору і контролю за інформаційної інфраструктурою Югославії. Нові стратегії проведення інформаційних операцій, продемонстровані США та їх союзниками по НАТО, засвідчили могутність інформаційних озброєнь розвинутих країн і необхідність міжнародного вирішення проблеми інформаційної безпеки [8].

– Модель С – наявність кількох країн–інфолідерів та потенційного протиборства між ними, визначення фактору стримування експансії інформаційних загроз, забезпечення в перспективі домінування однієї з держав у сфері міжнародної інформаційної безпеки з можливостями значного впливу на глобальну інфосферу та переважного права вирішення проблем глобального світового порядку.

Дослідження ЦРУ 90–х років та на перспективу до 2020 року визначали як основні джерела загроз в кіберпросторі для США тільки дві країни – Росію і Китай. У новій військовій доктрині збройних сил США (Концепція Force XXI, 1996 р.), де було запропоновано дві складові театру воєнних дій – традиційний простір і кіберпростір, основними

об'єктами впливу стали інформаційна інфраструктура і психологічна сфера (human network) противника [9].

На сучасному етапі експерти США відзначають, що стратегію різних видів інформаційних операцій, спрямованих проти країни, планують і здійснюють більше 20 країн світу, а конфронтуючі зі США держави включають інформаційну війну у свої воєнні доктрини. Тому стратегія «Force XXI» як фактор стримування експансії в міжнародному інформаційному просторі є інструментом інформаційної переваги США в глобальному протиборстві.

– Модель D – всі конфліктуючі сторони використовують транспарентність інформації для формування ситуативних альянсів, для досягнення переваг локальних рішень, які спроможні заблокувати технологічне лідерство, для використання можливостей інфоінфраструктури на окремих територіях з метою організації внутрішнього конфлікту між опозиційними силами (політичні, сепаратистські, міжнаціональні конфлікти) для проведення міжнародних антитерористичних інформаційних операцій.

У рамках міжнародної антитерористичної операції «Помста» (Афганістан, 2001 р.) мета спеціалізованих центрів США, відповідальних за проведення інформаційних операцій, полягала у плануванні психологічних кампаній, реагуванні на зміну ситуації, у підтримці інформаційних ресурсів та безпеки військових сил і цивільного населення. «США мали намір нейтралізувати і знищити всю терористичну мережу, яка загрожує Америці і решті цивілізованого світу, – заявив на прес–конференції для міжнародних мас–медіа тодішній держсекретар США К. Пауелл. – Мета операції «Помста» полягала не тільки у боротьбі проти тероризму, а й у переконанні певних режимів, які підтримують політику тероризму в тому, що така стратегія не відповідає їх власним інтересам. США задоволені реакцією світової спільноти та політичних лідерів більшості країн на пропозиції щодо глобальної боротьби з тероризмом».

Так, Північний Альянс вперше в історії застосував статтю 5 Статуту НАТО, яка спрямована на забезпечення загального захисту країн–членів перед викликами зовнішніх загроз; держави ЄС, країни–учасниці ГУАМ підтвердили підтримку дій США в акції «Помста» і консолідацію зусиль міжнародного співтовариства у протиборстві з міжнародним тероризмом у спільній заяві та меморандумі дій; прем'єр міністр Російської Федераціїї В. Путін запропонував розробити нову систему глобальної безпеки, враховуючи, що тероризм і його різновиди медіа– та кібертероризм стали глобальною загрозою для міжнародного миру у XXI ст.

Газета «USA Today» подає модель інформаційної війни проти режиму Талібан, яка включає проведення психологічної операції в інформаційному просторі Афганістану з одночасним блокуванням національних радіостанцій, поширенням пропагандистських матеріалів з уривками з Корану з метою протидії закликам до джихаду та формування у суспільній свідомості відчуття неодмінної перемоги антитерористичного альянсу в ході операції «Помста».

– Модель E – протиборство світової спільноти та міжнародної організованої злочинності, здатної контролювати перебіг політичних, економічних, суспільних і, зрештою, цивілізаційних процесів. Можливість такої моделі передбачена в дослідженні Національної ради розвідки США «Mapping the global future» – 2020 у версії «Коло страху» («Cycle of fear»), яка є найбільш песимістичним сценарієм майбутнього світової спільноти.

Враховуючи високу здатність інформаційних озброєнь до інтеграції з іншими традиційними і технологічно новими видами військових засобів, потенційні наслідки безконтрольного застосування багатошарового страту можуть виявитися катастрофічними для

існування людства. Тому тільки широке багатостороннє співробітництво може гарантувати світові вирішення нових складних проблем інформаційної доби і забезпечити реальну міжнародну інформаційну безпеку [2, с.17–22].

Особливість XXI століття – стрімкі переміни в усіх сферах життя, зміна декількох соціально–економічних систем, перед кожною із яких з часом з'являлися свої складнощі та обмеження. І той, хто керується застарілими поняттями, методами та теоріями, сам створює передумови для своєї поразки.

Одним із завдань інформаційно–психологічної війни є відірвати суспільну свідомість від реальності, змусити людей діяти неадекватно.

Заборонити розробку та використання інформаційної зброї неможливо. Обмежити зусилля багатьох країн з формування єдиного глобального інформаційного простору також нереально. Проте цілком можливо підписати розумні погодження, які б опиралися на міжнародне право та мінімізували загрозу застосування інформаційної зброї.

Концепція міжнародної інформаційної безпеки визначає критичні структури, які, в першу чергу, зазнають впливу в умовах інформаційного протиборства. Найбільш вразливими вважаються політична, суспільна, економічна, військова, науково–технологічна, духовна сфери життєдіяльності суспільства.

У політичній сфері інформаційна безпека стосується всіх елементів політичної структури держави та суспільства: структур підготовки та прийняття політичних рішень, структур управління місцевої та регіональної влади, структур виборчих систем, інформаційно–телекомунікаційних урядових систем спеціального призначення.

Перебіг міжнародних інформаційних операцій «Спільні зусилля» (1996 р.), «Союзницька сила» (1998 р.) свідчать про інтенсивний психологічно–пропагандистський тиск на політичного лідера Югославії С. Мілошевича та політичні структури країни з метою дискредитації югославського керівництва та заміни, як наголошувалося у зверненнях до населення СФРЮ, «військового злочинця» і передачі його Міжнародному трибуналу.

Ідеологічна операція «Perestroika» (1980–1990 рр.) підтвердила стратегію глобальних інформаційних операцій США у забезпеченні лідируючих позицій в системі міжнародної безпеки та світової політики. За словами Б. Клінтона, США , вплинувши на ідеологічні основи СРСР, вивели із війни за світову гегемонію державу – основного конкурента Америки, а наступні інформаційно–психологічні операції та політичні рішення були спрямовані на встановлення західної моделі демократії у нових державах Центральної та Східної Європи.

США здійснили потужний інформаційний вплив на світову громадську думку, виступаючи з жорсткими політичними заявами щодо президентських виборів у Республіці Білорусь (2001 р.). У заяві Білого Дому підкреслено, що «Лукашенко як останній диктатор Європи не лише викрав вибори у білоруського народу, він викрав у народу можливість повернутися на шлях демократії і ринкової економіки», тому США будуть співпрацювати з європейськими союзниками та міжнародними організаціями для захисту демократій і верховенства права в Білорусі різними засобами.

В економічній сфері критичними є системи загальноекономічного аналізу та прогнозування економічного розвитку, структури прийняття рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, системи управління в критично важливих для держави структурах (енергетика, комунікації, інформаційні мережі).

Досвід інформаційно–розвинутих країн свідчить, що економічні переваги ґрунтуються в сучасному світі на прогресивній інформаційній експансії, і саме ті країни, які

найбільше просунулися у напрямку інформаційної цивілізації, будуть переважати у світовій господарській системі та в міжнародній конкуренції з технологічно відсталими країнами та регіонами.

Відомий у світі Інститут аналізу фінансових ринків Дж. Сороса розробив і здійснив інтервенції в Азійсько–Тихоокеанському регіоні, Російській Федерації та Європі (1992, 1997, 1998 рр.), які супроводжувалися спеціальними інформаційно–психологічними операціями: виступи і заяви Сороса у «Financial Times» та інших мас–медіа про невизначеність валюти «євро», необхідність девальвації російського рубля, трансформацію ринку цінних паперів у Японії, про залежність німецької марки від девальвації фінансового ринку Росії. За оцінками європейських експертів, чистий прибуток Сороса в результаті інформаційної акції та інтервенції на ринках склав близько 300 млн. доларів.

Як елемент впливу на урядові структури Югославії було використано інформаційну загрозу превентивної економічної блокади. Держсекретар адміністрації Б. Клінтона з проблем зовнішньої політики М. Олбрайт з цього приводу заявила, що країни НАТО аналізують можливості обмеження поставок енергоносіїв в Югославію, а хакерам ЦРУ було поставлено завдання розкрити секретні рахунки С. Мілошевича в зарубіжних банках як для притягнення його до Міжнародного Суду за економічні злочини перед народом [2, с.22–24].

Корпоративні війни в інформаційній сфері позначені інтенсивним злиттям ТНК, домінуванням в інформаційному секторі світової економіки групи інформаційно–розвинутих країн, використанням стратегії інформаційного імперіалізму та значним обмеженням розвитку економічної системи країн незахідної цивілізації.

Суспільна сфера виступає найбільш вразливою для інформаційних впливів, оскільки включає системи формування громадської думки, структури ЗМК, інформаційно–організаційні структури політичних партій, громадських рухів, національно–культурних та релігійних інституцій, структури забезпечення основних прав і свобод, плюралізму і незалежності виявлення поглядів, вільного обміну ідеями та інформацією.

У рамках операції НАТО «Союзницька сила» було застосовано засоби впливу проти інфоінфраструктури Югославії, проурядових ЗМК, системи формування громадської думки: від бомбардування телерадіостанцій, жорсткого контролю національного інформаційного простору, заборони на мовлення в аналоговому форматі до заміни і виведення інформаційного простору за межі національної території за допомогою технологій Internet і створення нової інформаційної реальності для національного суспільства.

Сербський парламент у відповідь на загострення косовської кризи прийняв Закон про суспільну інформацію, за яким було заборонено трансляцію зарубіжних програм на території країни через національні канали комунікації. Зокрема, дискримінаційні штрафи, які потрібно було сплатити протягом доби, і заборона інформаційної і професійної діяльності торкнулися таких засобів масової комунікації, як «Danas», «Nasa Borba», «Dnevni Telegraf», «Europ/Janin» [2, с.24–25].

Глобального характеру набули інформаційні загрози в науково–технологічній сфері: від феномену транскордонного переміщення інтелектуальних ресурсів, тобто вивезення інформації унікального науково–технологічного характеру на біологічних носіях до міжнародних систем спостереження, аналізу та прогнозування тенденцій науково–технологічного розвитку з метою доступу до конфіденційних баз і банків даних.

Критичними для безпеки у сфері науки та технологій є структури накопичення науково–технічної інформації, інституції та структури фундаментальних і прикладних досліджень, об'єкти інтелектуальної власності, ноу–хау. Інформаційно–технологічний аспект

безпеки зорієнтований на реалізацію системних заходів, спрямованих на максимальне вдосконалення науково–технологічної сфери, ефективний захист інтелектуальних ресурсів. Проблема інформаційної безпеки тісно пов'язана з діяльністю промислової розвідки, несанкціонованим втручанням у конфіденційні мережі та системи, кібервійнами спецпідрозділів окремих країн, конкуренцією на світових ринках.

Відомими стали інформаційні операції в галузі цифрового мобільного телебачення, «нейронних» комп'ютерів, новітнього програмного забезпечення, біотехнологій Японії, США, Ізраїлю, де системи аналізу науково–технологічної інформації є елементом державної політики та доктрини воєнної безпеки.

Аналіз системи наукових грантів, які поширювалися в Україні зарубіжними фондами, свідчить про особливу зацікавленість провідних країн світу до науково–технологічних розробок Інституту Патона, Інституту надтвердих матеріалів, Інституту біотехнологій тощо. З одного боку, це свідчить про наявність інтелектуального потенціалу України, з іншого, про міжнародну конкуренцію з боку західних країн у галузі високих технологій та наукових досягнень [2, с.25–26].

У військовій сфері вразливими в умовах інформаційного протиборства вважаються інформаційні ресурси збройних сил, ВПК, системи управління військами, системи контролю і постійного спостереження, канали надходження інформації стратегічного, оперативного, розвідувального характеру. Наприклад, США використали свої інформаційні можливості за допомогою системи «Echelon» (код 1947 «UKUSA Agreement») для виявлення програми розробки ядерної зброї в Кореї і для укладення детальної угоди з її ліквідації; для оперативного з'ясування і попередження співробітництва Росії та Китаю з Іраном в ядерній та ракетній галузях: для забезпечення механізму контролю ООН з інспектування іранських ядерних об'єктів, а також для вивезення ядерного потенціалу і тактичної зброї з України, викриття контракту «Thomson CSF» – поставки французької зброї до Бразилії, операції з відмивання грошей за продаж зброї в треті країни.

Система «Echelon» і нова система спостереження і перехоплення комунікацій «Око світу» як засіб доступу до будь–яких видів інформації у глобальному вимірі (телекомунікаційні мережі і системи, супутниковий, мобільний та високочастотний зв'язок, Internet) орієнтовані на перехоплення інформації урядових, комерційних, приватних структур в будь–якому регіоні світу. За допомогою системи здійснюється доступ до всіх основних компонентів глобальної інфоінфраструктури.

Під час операції «Союзницька сила» у відповідь на бомбардування інфраструктури Югославії сербські хакери заблокували за допомогою атаки ping of death офіційний сервер НАТО, ряд інших військових та урядових сайтів країн–членів Альянсу повідомленнями з макровірусами, що підтвердило прогнози про перенесення військових операцій у кіберпростір, на рівень інформаційного протиборства. А керівництво СФРЮ розсекретило через мережу Internet інформацію про американський план «Корені», яким планувалася етнічна та воєнна дестабілізація на Балканах з метою закріплення тенденції необоротних змін на посттоталітарному просторі.

Духовна сфера стає критичною в умовах конфесійного протистояння, релігійного фанатизму, трансформації духовних ідеалів та морально–етичних цінностей. Проявом критичності духовної сфери (Ірландія, Алжир, Ізраїль, Афганістан, Китай, Іран) на міжнародному рівні стала проблема, пов'язана з рішенням керівництва ісламського радикального руху «Талібан» (Афганістан) про руйнування неісламських релігійних пам'яток, що віднесені до глобальної культурної спадщини і перебувають під охороною ЮНЕСКО.

До сучасних інформаційних загроз відносять також кібер–, медіа– та психотероризм як протиправні дії, спрямовані на руйнування життєво важливих інфраструктур, систем управління державою, морального стану суспільства та війська, порушення прав людини [2, с.27].

Підсумовуючи наведені спостереження, можна зробити наступні висновки: спроможність країни боротися с сучасними інформаційними загрозами впливає на її образ на міжнародній арені. Феномен міжнародної інформаційної безпеки обумовлюється стратегічною спрямованістю інформаційних озброєнь проти критично важливих структур життєдіяльності і функціонування міжнародного співтовариства, визнання інформаційної зброї як нового глобального виду зброї масового ураження, катастрофічного за наслідками свого застосування (деякі дослідники називають інформаційні озброєння «інформаційним апокаліпсисом»).

Таким чином, поняття міжнародної інформаційної безпеки є вагомою складовою геополітичного образу країни у сфері міжнародних відносин і проявом тенденцій нових глобальних викликів і глибинних процесів.

.

Література

1. Замятин Д.Н. Географические образы в гуманитарных науках [Електронний ресурс]. – Режим доступу: http://www.courier.com.ru/homo/zip/media.zip 2004
2. Міжнародна інформаційна безпека : Сучасні виклики та загрози [Текст]. – К.: Центр вільної преси, 2006. – 916 с.
3. Гриняев С. Эксперты корпорации «РЭНД» об информационной стратегии Електронний ресурс . – Режим доступу: http://attend.to/commi.
4. Юдін О.К. Інформаційна безпека держави: Навчальний посібник [Текст] / О.К. Юдін, В.М. Богуш. – Х.: Консум, 2005. – 576 с.
5. Пухова Калерия. Совбез занялся СМИ: Доктрина информационной безопасности может сработать против российских масс–медиа http://www.ng.ru/printed/8786.
6. Nye J.S. America's Informational edgel Strategy and force planning [Електронний ресурс]. – Режим доступу: http://ics.leeds.ac.uk/papers/vp01.cfm?outfit= pmt&requesttimeout =500&folder=49&paper=155
7. Леваков А. В США готовятся к защите информационных систем [Електронний ресурс]. – Режим доступу: http://ww–4.narod.ru/index.html
8. Гриняев Сергей. Особенности информационной войны во время агрессии НАТО против Югославии (по материалам открытой печати) [Електронний ресурс]. – Режим доступу: http://ww–4.narod.ru/warfare/grinyaev/page008.htm
9. Гриняев С.Н. Информационная война: история, день сегодняшний и перспектива [Електронний ресурс]. – Режим доступу: http://ww–4.narod.ru/warfare/grinyaev /page009.htm
10. Арон Раймон. Мемуары: 50 лет размышлений о политике [Текст] = Memoires: 50 Ans de Reflexion Politique / Р. Арон; пер. с фр. Г.А. Абрамова, Л.Г. Ларионовой. – М.: Ладомир, 2002. – 873 с.