УДК 1:316.4

Дзьобань О. П., Панфілов О. Ю., Чемчикаленко Р. А.

ІНФОРМАЦІЙНІ АСПЕКТИ БЕЗПЕКИ У СОЦІОКУЛЬТУРНИХ ПРОЦЕСАХ

Анотація. *У статті розкриваються інформаційні аспекти безпеки сучасного суспільства та його соціокультурних процесів. Показано, що усі складові інформаційної безпеки є невід'ємними й системотворчими в інших видах безпеки. Констатується, що інформаційна безпека пронизує всі види безпеки і її забезпечення є пріоритетним завданням. Розглядається роль інформаційної безпеки в економічних процесах та процесах забезпечення обороноздатності держави. Висвітлено роль інформаційної війни та інформаційного тероризму у створенні інформаційних небезпек у соціумі. Обґрунтовується, що на сучасному етапі розвитку суспільства без забезпечення інформаційної безпеки практично неможливо забезпечити ніякий інший вид безпеки й національну безпеку країни в цілому. Запропоновано нову типологію основних груп загроз суспільству в інформаційній сфері.*
Ключові слова: *інформаційна безпека суспільства, соціальна безпека, інформаційна війна, інформаційний тероризм, загрози інформаційній безпеці.*

Постановка проблеми. Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що є сукупністю інформаційних ресурсів, інформаційної інфраструктури, системи формування, розповсюдження й використання інформації, а також системи регулювання виникаючих при цьому суспільних відносин. У даний час багато найважливіших інтересів людини, суспільства, держави в значній мірі визначаються станом оточуючої їх інформаційної сфери. Тому можна припустити, що інформаційна безпека може розглядатися як найважливіший компонент національної безпеки, який «пронизує» усю решту видів безпеки.

Результати авторського **аналізу останніх досліджень** свідчать, що глобальна інформатизація суспільства, стрімкий розвиток інформаційної техніки й нових інформаційних технологій, збільшення потреб суспільства в різноманітних інформаційних послугах, формування в останні десятиліття національних і глобальних інформаційно-телекомунікаційних систем привело до появи нового виду економіки – інформаційної [5, 10]. Разом з тим, місце й роль інформаційних аспектів безпеки особистості, суспільства й держави і до сьогодні залишаються чітко невизначеними.

Необхідно зазначити, що дослідженням сутнісних та змістовних основ інформаційної безпеки присвячені праці Р. Абдєєва, В. Афанасьєва, Т. Берези, Е. Бєлясова, М. Буслепка, В. Глушкова, С. Гриняєва, О. Данильяна, О. Дзьобаня, Г. Смельянова, М. Кастельса, В. Лекторського, В. Лисицького, В. Лопатіна, Й. Масуди, А. Мінка, Е. Моргунова, Дж. Нейсбіта, Б. Парахонського, Е. Паркера, Г. Почепцова, А. Ракітова Е. Тоффлера, В. Циганкова, М. Чеснокова та інших дослідників.

Метою статті є концептуальне визначення місця й ролі інформаційних аспектів у забезпеченні безпеки людини, суспільства й держави.

Основні результати дослідження. Пріоритетність того або іншого виду безпеки визначається наступними чинниками:

- потребою громадян, суспільства, держави і світової спільноти;
- зростаючою уразливістю людей і життєво важливих об'єктів держави без зосередження зусиль на зміцненні даного виду безпеки;
- наявністю широкого кола небезпек і загроз, яким повинна протистояти дана система безпеки. Очевидно, що власне інформаційної безпеки стосуються всі ці чинники.

Глобальна інформатизація суспільства, стрімкий розвиток засобів інформаційної техніки й нових інформаційних технологій, збільшення потреб суспільства в різноманітних інформаційних послугах, формування в останні десятиліття національних і глобальних інфор-

маційно-телекомунікаційних систем привело до появи нового виду економіки – інформаційної економіки.

Інформаційна економіка включає наступні основні компоненти: виробництво засобів інформаційної техніки, включаючи засоби зв'язку і передачі даних; виробництво інформаційних продуктів і інформаційних ресурсів; надання інформаційних послуг користувачам. Інформаційна економіка впливає практично на всі сторони суспільного розвитку [10]. Розвиток інформаційної економіки і місце тих або інших країн у новому глобальному інформаційному просторі набувають вирішального значення в геополітиці розвинених країн. Саме тому розвитку інформаційної економіки як стратегічно важливому напряму соціально-економічного розвитку суспільства сьогодні приділяється першорядна увага в таких країнах, як США, Японія, ФРН, Франція, Велика Британія. Загальновідомо, що успіхи, що спостерігаються останніми роками, в розвитку економічної могутності цих країн досягнуті завдяки їх все більш рішучій орієнтації на розвиток інформаційної економіки. У таких умовах національну безпеку держави в принципі не можна забезпечити без розвиненої інформаційної економіки.

Основу інформаційної економіки розвиненої держави складають інформаційні ресурси. Поняття національних інформаційних ресурсів сьогодні претендує на роль нової економічної категорії. Пріоритетний характер інформаційних ресурсів в суспільстві робить особливо актуальною проблему їх захисту. Збиток, що наноситься тим або іншим способом інформаційним ресурсам держави, безпосередньо торкається інтересів економічної безпеки.

В даний час взаємозв'язок різних країн планети є таким, що люди практично всіх країн потребують знань, культури, мистецтва і науки, що знаходиться за кордоном. Але якщо це так, то повинні бути цивілізовані правила обміну в цих сферах, які підсилюватимуть, а не обмежуватимуть подальші інновації. Створити такі правила, а також інформаційну етику, яка лежить в їх основі – це виключно важке для вирішення завдання в світі, розділеному на три частини, в кожній з яких переважає або сільське господарство, або індустріальна, або постіндустріальна економіка. В той же час очевидно, що ці проблеми мають тільки одну тенденцію – ставати все більш важливими.

Відзначимо, що створення планетарного інформаційного простору за допомогою глобальних комп'ютерних мереж може мати серйозні наслідки для національної, зокрема економічної безпеки. Інформаційний простір не має державних кордонів, не має таких інститутів захисту державних інтересів, якими є прикордонна й митна служби, поки що відсутні способи і засоби контролю цінності і важливості інформаційних ресурсів, що «перевозяться» через кордон. Поки що державний кордон є практично прозорим для інформаційних ресурсів.

Впровадження інформаційних і телекомунікаційних технологій, оснащення ними державних структур ставить проблему захисту інформації і елементів інформаційного забезпечення на абсолютно пріоритетний рівень.

Особливо важливою ця проблема стає у зв'язку з використанням глобальних інформаційних мереж в держструктурах. Так, загальнодоступність мережі Інтернет, її відкритість, наявність величезного числа програмних засобів, розроблених в різних країнах світової спільноти, можуть представляти небезпеку для економічної безпеки країни і національної безпеки в цілому. Зокрема, несанкціонований доступ через глобальну інформаційну мережу в бази даних державних структур з метою їх руйнування, цілеспрямованого спотворення або використання інформації в злочинних цілях може завдати серйозного збитку державі. Особливо гостро проблеми розробки методів захисту власних інформаційних ресурсів у відкритих мережах встають перед країнами, які технологічно відстають у сфері інформаційних і телекомунікаційних технологій від США або Західної Європи. До таких країн, на жаль, відноситься й Україна.

Тому, з одного боку, слід строго стежити за тим, щоб інформація, що становить державну таємницю, не розміщувалася в Інтернет і на робочих місцях користувачів, які працюють із закритою інформацією, а з іншого – аргументовано відносити інформацію до категорії закритої, не включаючи в цю категорію велику кількість документів, що формуються відкри-

тими комерційними структурами, ЗМІ і т.п. Кожна держава повинна мати методи захисту своїх життєво важливих інтересів. Тому, певна частина знань, наявних у тій або іншій державі, буде завжди закрита для доступу, якщо ці знання пов'язані з питаннями безпеки держави.

При проведенні комплексної державної політики у сфері інформаційної безпеки і з метою підтримки вітчизняних виробників необхідним є введення гнучких диференційованих обмежень на подальше збільшення в українських телекомунікаційних системах зарубіжних цифрових комунікаційних засобів, а також створення умов пріоритетного розвитку вітчизняних розробок і виробництв у сфері сучасних телекомунікацій і програмного забезпечення з метою поступового заміщення зарубіжного телекомунікаційного устаткування зі сфер, що забезпечують національну безпеку України [2].

Актуальною є також проблема методів захисту існуючих інформаційно-телекомунікаційних технологій. Розвиток інформаційних і телекомунікаційних систем, їх широке впровадження у всі сфери життєдіяльності суспільства призводить до зростання залежності суспільства, окремої людини від безперебійного функціонування даних засобів, від гарантій використання накопичуваної в них інформації в інтересах громадян, що не суперечить законним інтересам, суспільства і держави. Очевидно, що помилки в роботі інформаційних систем управління повітряними перевезеннями, рухом залізничного транспорту тощо можуть послужити причиною великих трагедій і величезного матеріального збитку, не говорячи вже про системи управління небезпечними виробництвами, АЕС, стратегічною ядерною зброєю. Все це дозволяє зробити висновок про те, що складові інформаційної безпеки є центральними для національної безпеки.

Сьогодні особливу важливість в оборонній сфері відіграє інформаційна структура оборонного потенціалу країни, роль і значення якої постійно зростає. Всі сучасні засоби озброєння, системи управління військами і зброєю є системами критичних додатків (так прийнято називати системи, порушення функціонування яких призводить до різкого ослаблення безпеки держави) з високим рівнем комп'ютеризації. Ці системи можуть виявитися вельми уразливими, зокрема, з точки зору дії інформаційної зброї як у воєнний, так і в мирний час [12]. Уразливість систем критичних додатків може призвести до того, що зброя країни за допомогою прихованого впровадження в програмне забезпечення систем управління цією зброєю «програмних закладок» виявиться повністю або частково виведеною з ладу. Зокрема, про реальність цього твердження свідчить досвід війни в Перській затоці. Ірак практично не зміг застосувати куплені у Франції системи протиповітряної оборони, тому що їх програмне забезпечення містило «логічні бомби», які були активізовані з початком бойових дій.

Таким чином, оборонну безпеку держави неможливо забезпечити без відповідного рівня розвитку інформаційних технологій. Для цього вже недостатньо швидко розробляти власні програмні засоби й інші технології, необхідні науковий потенціал і відповідні методології, які дозволять створювати у випереджаючому ритмі принципово нові і якісні засоби – такі як «генетичні» програми, «генетичні» шифри і т.п.

Як уже наголошувалося вище, зараз реальністю став новий тип війни – інформаційна війна. Ефективність протидії інформаційній зброї визначатиметься методами і формами використання інформаційного ресурсу як зброї. Таким чином, суть інформаційної війни полягає в боротьбі за допомогою інформації проти інформації. Як відзначав Е.Тоффлер, контроль над знаннями – ось суть майбутньої всесвітньої битви за владу у всіх інститутах [16].

Театр воєнних дій розширюється до таких глибин, які іноді називають «дух цивілізацій», тобто все більше переміщається у сферу духовну, в зіткнення базових цінностей, цілей, знань, теорій. Більше того, у разі швидкого й масового перепрограмування нації в процесі інформаційної війни, найбільш ефективними є прийоми, що мають емоційне забарвлення і що належать таким сферам, як масова культура, мистецтво, релігія і т.п. На нашу думку, певні методи такого перепрограмування були успішно застосовані проти СРСР, що призвело до його розпаду. Таким чином, цілеспрямований односторонній вплив на духовні цінності і на їх носіїв не є нешкідливим для окремої людини, нації і людства в цілому. Слід зазначити, що

наслідком такої війни стає знищення різноманітності культур, що неминуче веде до зупинки розвитку людства [4].

Для руйнування суспільної системи в першу чергу потрібно зруйнувати найбільш значущі зв'язки, систему взаємодії між ключовими елементами і структурами соціальної системи, приводячи її в стан, близький до хаотичного. Дослідження у галузі синергетики показують, що в будь-якій складній системі, що саморозвивається, генетично закладений механізм саморуйнування. Цей механізм має інформаційну основу і є уразливим з боку зовнішніх інформаційних дій. Тому найбільш результативними є такі інформаційні дії, які активізують саме механізми саморуйнування, вражаючи в першу чергу систему управління суспільством, яка, у свою чергу, сама продовжуватиме руйнування соціальної системи, держави.

Дослідження у галузі синергетики також показали, що в певні моменти часу (точки біфуркації) складна система, якою є суспільство, стає вельми нестійкою. Вона стає дуже чутливою до зовнішніх інформаційних дій, навіть якщо вони є дуже слабкими у порівнянні з інформаційним потенціалом самої системи. Саме ця властивість і використовується при веденні інформаційної війни.

Більшість вчених вважає, що в сучасних умовах і у перспективі вони здійснюватимуть надзвичайно суттєвий вплив на перебіг і результати як протистоянь, так і конфліктів та воєн різної інтенсивності. Інформаційні технології, засоби масової комунікації багаторазово посилили можливості психічного впливу на людину, групи людей і населення країни в цілому. За оцінками психологів «людина розумна» поступово перетворюється в «інформаційну людину». Поряд з традиційними методами керування суспільством, колективами та окремими особами (адміністративно-організаційні, економічні, соціально-психологічні та правові) усе більше розповсюдження отримує спеціальний метод централізованого впливу на широкі кола населення – метод інформаційного керування. Методологічною основою інформаційного керування у значній мірі є настанова Антоніо Грамші, в основі якої лежать положення про те, що для досягнення стратегічної мети зміни суспільного ладу треба діяти, змінюючи не базис суспільства, а через надбудову – силами інтелігенції (здійснюючи «молекулярну агресію» у свідомості суспільства і руйнуючи його культурне ядро). Ці положення узгоджуються з одним із базових постулатів теорії управління, який проголошує, що значно легше досягти еволюції у свідомості людини, аніж здійснити у ньому революційні зміни [8, с. 238].

Основними засобами досягнення таких цілей при цьому є засоби масової інформації (ЗМІ), освітні системи та культові утворення, а також найбільш підвладні такому впливу підлітки та молодь. Так, у США з 50-их років XX століття інтенсивно проводяться розробки методів і засобів спеціального впливу на психіку. З 70-их років дослідні програми проводяться у кращих лабораторіях університетів усього світу: США, Німеччини, Австрії, Франції, Італії, Японії, Ізраїлю, Китаю та інших. До цілей поразки психіки людини відносять [9, с. 240]:

– перекручення інформації, отриманої політичним керівництвом, командуванням та особовим складом збройних сил супротивника і нав'язування їм хибної або беззмістовної інформації, яка позбавляє їх можливості правильно сприймати події або поточну обстановку і приймати вірні рішення;
– психологічна обробка військ та населення;
– ідеологічні диверсії;
– пропаганда;
– зміна і керування індивідуальною та колективною поведінкою.

Суттєвою небезпекою для сучасного суспільства постає інформаційний тероризм або кібертероризм.

Останні досягнення у сфері інформатизації й телекомунікацій значно розширили арсенал терористичних засобів і методів, а також ефект їх дії. Сьогодні міжнародний тероризм володіє значно ширшими технологічними можливостями, аніж 10–15 років тому. Разом з традиційними видами залякування, терористи в своєму арсеналі широко використовують комп'ютерні технології й Інтернет. Так, секта «Аум Синрікьо» працювала над створенням

електромагнітних імпульсних «гармат», що виводять з ладу комп'ютерні системи, проводила експерименти зі створення нових небезпечних мережевих вірусів, а також вела набір нових рекрутів у свою секту з використанням Інтернет. У 2000 році ця секта мала офіційні контракти на розробку програмного забезпечення для 80 японських компаній і 10 урядових агентств, включаючи Поліцейський департамент японського метрополітену [18].

На початку 2003 роки під новим для терористів гаслом – «поставити на коліна Інтернет» – оголосив про себе як про нову терористичну організацію «Арабський Електронний Джихад» (AEJT) [11]. Організація AEJT заявила про те, що збирається знищити всі ізраїльські й американські Інтернет-сайти, а також усі інші неугодні їй сайти.

В інформаційному просторі можуть бути використані різні прийоми досягнення терористичної мети. В їх числі [15]:

– нанесення збитку окремим фізичним елементам кіберпростору, наприклад, знищення або активне придушення ліній зв'язку, руйнування мереж електроживлення, наведення перешкод, використання спеціальних програм, стимулюючих руйнування апаратних засобів тощо;

– несанкціонований електронний доступ до критичних елементів кіберпростору, модифікація або знищення інформаційного, програмного або технічного ресурсів;

– розкриття або загроза розкриття таємної інформації, зокрема про функціонування інформаційної інфраструктури держави;

– загроза здійснення терористичного акту в кіберпросторі, що спричиняє серйозні організаційні й економічні наслідки;

– захоплення каналів ЗМІ з метою розповсюдження дезінформації, демонстрації потужності терористичної організації й оголошення своїх вимог;

– інформаційно-психологічний вплив на населення, представників владних структур, операторів і розробників інформаційно-комунікаційних систем, а також фахівців з їх експлуатації.

Об'єктами кібертероризму є [21]:

– устаткування, включаючи комп'ютери, периферійне, комунікаційне, теле-, відео- й аудіоустаткування;

– програмне забезпечення;

– мережеві стандарти і коди передачі даних;

– інформація, яка може бути представлена у вигляді баз даних, аудіо-, відеозаписів, архівів тощо;

– фізичні особи.

Інформаційно-комунікаційні технології (ІКТ) стають вельми привабливим засобом здійснення терористичних актів. Це пов'язано з декількома чинниками [21]:

– доступністю й дешевизною ІКТ в порівнянні з іншими терористичними засобами;

– високою вражаючою здатністю ІКТ при їх терористичному використанні, особливо у разі спрямованості проти об'єктів критичної національної інфраструктури, яка сьогодні практично повсюдно ґрунтується на комп'ютерних системах і технологіях і часто виявляється пов'язаною мережею Інтернет, стаючи зручною «мішенню» для кібертерористів;

– можливістю здійснення екстериторіальних атак, зокрема з «інформаційних сховищ»;

– можливістю скоєння злочинів у режимі «он-лайн» і швидкого приховання слідів злочинів, спрямування органів, що здійснюють оперативно-розшукові заходи по помилкового сліду;

– меншим ризиком бути виявленими й ідентифікованими при здійсненні кібератак, особливо в умовах багатократного посилювання останнім часом у багатьох країнах заходів забезпечення фізичної безпеки ключових об'єктів інфраструктури;

– високою вірогідністю того, що терористи залишаться безкарними або понесуть легке покарання за діяння, які, будучи здійснені поза інформаційним простором, жорстко караються;

– унікальною можливістю таємно, планомірно й ефективно впливати на індивідуальну й масову свідомість, громадську думку, процеси ухвалення рішень; поширювати пропагандистські матеріали для вербування в свої ряди або отримання політичної підтримки своєї діяльності; проводити дезінформацію, викликати паніку.

Крім того, ІКТ, зокрема Інтернет, дозволяють терористичним групам більшість з яких має в даний час мережеву організаційну структуру, ефективно і таємно здійснювати зв'язки між її розрізненими осередками і окремими членами, проводити збір засобів (коштів) та інформації про майбутні цілі.

Дії кібертерористів можуть бути направлені на критичні інформаційні об'єкти військової (оборонної) й цивільної інфраструктури. Так, в атомній енергетиці зміна інформації або блокування інформаційних центрів може спричинити припинення подачі електроенергії в міста й на військові об'єкти, викликати ядерну катастрофу. Спотворення інформації або блокування роботи інформаційних систем у фінансовій сфері можуть призвести до економічної кризи, а виведення з ладу систем управління військами й військовою технікою – спровокувати початок бойових дій, стати причиною втрат серед цивільного населення й військових. Колосальні людські втрати й екологічна криза можуть бути результатом терористичного втручання в роботу транспортних систем, об'єктів біологічної або хімічної промисловості.

Особливу небезпеку представляє кібертероризм при аваріях, катастрофах і стихійних лихах, оскільки приховування, затримка надходження, спотворення й руйнування оперативної інформації, несанкціонований доступ до неї окремих осіб або груп осіб можуть призвести як до виникнення складнощів при ліквідації наслідків надзвичайної ситуації (приведення в рух великих мас людей, що під впливом психічного стресу; швидке виникнення й розповсюдження серед них паніки і безладів на основі чуток, помилкової або недостовірної інформації), так і безпосередньо до людських жертв.

Терористам, як і хакерам, доступні програмні засоби інформаційного впливу (віруси, «черв'яки», «троянські коні» та інші програми, що містять шкідливі коди). Проте, їх використання може бути максимально дієвим тільки за наявності програмного забезпечення, на яке здійснюється напад, неусунених на момент атаки недоробок і «вузьких місць» у програмах і алгоритмах. Разом з комп'ютерними засобами для терористів доступними стали могутні випромінювачі електромагнітних полів, створення яких виявилося можливим завдяки розвитку високоточної й високовольтної електротехніки. Такі електромагнітні випромінювачі є високоефективним і доступним засобом деструктивного впливу на інформаційний простір. їх використання в терористичних цілях одержало назву «електромагнітний тероризм» [1].

За оцінками експертів, терористи вже сьогодні здатні використовувати такі засоби електронної дії, як, наприклад, високопотужна мікрохвильова зброя. Вона може ефективно застосовуватися проти будь-яких, зокрема чудово захищених комп'ютерів і електронного устаткування, причому, її застосування буде найбільш ефективним, перш за все, в розвинених країнах. Критичні інформаційні інфраструктури також є дуже вразливими для засобів електромагнітного імпульсного впливу [20].

Експерти вважають, що інформаційний тероризм може супроводжувати «традиційні» терористичні дії, оскільки порушення в роботі, наприклад, систем зв'язку або інформаційних мереж критичних інфраструктур країни можуть підсилити їх ефект і викликати паніку у суспільстві [15, 19]. Крім того, такі порушення можуть серйозно ускладнити проведення відповідних робіт після теракту.

Цілком очевидно, що в даний час проблема інформаційного тероризму є найбільш актуальною для постіндустріальних, найбільш розвинених в інформаційному плані, країн.

Отже, можна зробити висновок про те, що в сучасних умовах оборонна безпека держави у величезному ступені залежить від забезпечення її інформаційної безпеки.

Наступною проблемою в контексті даної статті є проблема соціальної безпеки, яка була й залишається однією з найважливіших [13-14]. Вона пов'язана із захистом інтересів країни і народу в соціальній сфері, розвитком соціальної структури і відносин у суспільстві,

системи життєзабезпечення і соціалізації людей, способу життя відповідно до потреб прогресу нинішніх і майбутніх поколінь.

Сучасні інформаційні технології дозволили різко підвищити ефективність засобів інформаційного впливу на психіку людей і суспільну свідомість, створити нові форми прихованого маніпулювання індивідуальною, груповою і масовою свідомістю. Як головна мета інформаційного впливу виступає людина, різного роду соціальні утворення та інститути. Докорінна деформація соціальної сфери за допомогою інформаційних засобів полягає в провокації крайнього соціального розшарування населення шляхом порушення прав при розподілі благ і послуг; розкладанні інститутів, призначених для всебічного розвитку особистості; розпалюванні національно-етнічної ворожнечі і т.д., що показує істотний вплив інформаційних процесів на соціальну безпеку. Багато результатів подібної інформаційної агресії в соціальній сфері вже є досить відчутними в даний час в Україні.

Особливо слід зазначити величезні можливості інформаційного впливу на особистість засобів масової інформації. По суті сьогодні ЗМІ – практично єдина структура, через яку населення щодня, щогодини одержує інформацію про процеси в регіоні, країні, світі, за допомогою якої населенню буквально нав'язують різні ідеологічні установки. Тому, особливо важливими є якість і достовірність інформації, що транслюється через ЗМІ. В даний час ЗМІ можуть виступити і як сила, що стабілізує обстановку в суспільстві, і стати детонатором соціального вибуху. Таким чином, соціальна безпека країни не може бути забезпечена без інформаційної безпеки.

Інформаційна безпека безпосередньо пов'язана і з екологічною безпекою. Сьогодні під екологічною безпекою розуміють стан захищеності особистості, суспільства, держави й навколишнього природного середовища від реальних або потенційних загроз антропогенного або природного походження, які впливають на біосферу [6-7]. Проблема екологічної безпеки є сьогодні однією з найважливіших проблем глобального масштабу. Вирішення більшості екологічних проблем і завдань пов'язане із збором і обробкою інформації про стан природного середовища (екологічний моніторинг), з моделюванням глобальних процесів природних явищ з урахуванням зростаючих техногенних дій і антропогенних навантажень. Найбільш ефективне все це може використатися тільки з використанням сучасних інформаційних і телекомунікаційних технологій.

Кардинальне поліпшення екологічної ситуації можливе тільки в умовах докорінної перебудови економіки за допомогою її інформатизації, висунення інформаційного ресурсу на місце пріоритетного ресурсу, що демонструє вплив інформаційної сфери на екологічну безпеку. У цих умовах наукова інформація і засоби інформатики виявляються тим інтенсифікаційним чинником, який реалізує оптимальні з екологічного погляду речовинно-енергетичні технології і тим самим інформатизація стимулює і прискорює процеси екологізації. Інформаційна економіка є менше природоємною, аніж економіка індустріального суспільства і є основою становлення інформаційного суспільства, в якому небезпека екологічної катастрофи буде значно зменшена. Таким чином, країна, що має високий рівень інформатизації, здатна не тільки досягти економічного розвитку, але й успішно вирішувати екологічні проблеми.

Інформаційне суспільство розглядається тут як завершальна стадія моделі нестійкого розвитку й одночасно як початкова стадія моделі стійкого розвитку, в якій тільки й можливе повне забезпечення екологічної безпеки. На думку Л. Урсула, перехід до стійкого розвитку і становлення інформаційного суспільства – це єдиний синергетичний процес виживання цивілізації [17]. Таким чином, тісний зв'язок екологічної і інформаційної безпеки є очевидним.

Одним з методів комплексного розгляду суті і змісту небезпеки і безпеки є діяльнісний підхід. Згідно з цим підходом забезпечення безпеки розглядається як суб'єкт-об'єктна взаємодія, в якій можна виділити й інші компоненти – цілі, потреби, умови, засоби і методи і т.д.

З позицій діяльнісного підходу, вплив небезпеки на ту або іншу систему є певним процесом. Виділяється статичний аспект даного процесу, який включає [3]:

– джерело або суб'єкт небезпеки;

– об'єкт, що наражається на небезпеку;

– засоби і методи, якими джерело небезпеки впливає на об'єкт інформаційного процесу або інформаційну систему.

Джерелом небезпек, як показав аналіз негативних ефектів інформатизації, може бути стихійне розгортання процесу інформатизації в моделі нестійкого розвитку, що призводить до деформації згаданого процесу і до інших негативних ефектів. Об'єктами, що наражаються на небезпеки, пов'язаними з таким процесом інформатизації, є люди і їх об'єднання (державні, політичні, економічні, суспільні, релігійні та ін. організації), суспільство в цілому, а також держава. Засоби і методи впливу суб'єкта небезпеки на об'єкт небезпеки різноманітні, але всі вони обумовлені особливостями моделі нестійкого розвитку суспільства, його негативними тенденціями, небезпеками і реальними і потенційними загрозами.

Традиційний підхід до визначення загроз інформаційній безпеці суспільства приводить звичайно до виділення наступних основних груп таких погроз.

Перша група загроз пов'язана з бурхливим розвитком нового класу зброї – інформаційної, яке здатне ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства і армії.

Друга група інформаційно-технічних загроз для особистості, суспільства й держави – це новий клас соціальних злочинів, заснованих на використанні сучасної інформаційної технології (махінації з електронними грошима, комп'ютерне хуліганство і ін.).

Третя група інформаційно-технічних загроз – електронний контроль за життям, настроями, планами громадян, політичних організацій.

Четверта група інформаційних загроз – використання нової інформаційної технології в політичних цілях.

Не заперечуючи корисності такої систематизації інформаційних загроз, ми вважаємо її все ж таки принципово недостатньою. Всі перераховані вище загрози визначаються на основі виділення різних способів використання інформації і інформаційної техніки в сучасному суспільстві, тоді як ширший і плідний, на нашу думку, підхід пов'язаний з розумінням суспільства як певної системи, яка не тільки використовує, але й проводить інформацію і інформаційну техніку. Саме виробничий підхід до інформаційних процесів здатний дати найбільш адекватну і повну картину як самого інформаційного суспільства, так і різних загроз його безпеці.

Запропонований нами підхід до аналізу системи інформаційного забезпечення і інформаційної безпеки суспільства, дозволяє виділити перш за все наступні основні групи загроз.

Загрози, пов'язані з руйнуванням або деградацією базисної інформаційної підсистеми суспільства, що забезпечує збереження і розвиток його інформаційно-культурного ядра. Реальним носієм і хранителем цього ядра є система освіти і виховання нових поколінь суспільства. Реальною загрозою для неї є, з одного боку, недостатня увага самого суспільства до захисту і не завжди благотворний інформаційний вплив на цю систему з боку інших суспільств, зацікавлених в її трансформації у прийнятний для них бік.

Загрози, пов'язані з руйнуванням або деградацією динамічної продуктивної інформаційної підсистеми суспільства. Реальними виробниками у цій сфері є всі наукові, інженерно-технічні, аналітичні, ідеологічні і художньо-культурні центри, що виробляють або імпортують відповідну інформаційну продукцію й інформаційну техніку.

Загрози науково-теоретичного забезпечення суспільства. Йдеться про діяльність науковців та науковий потенціал нації, якій внаслідок руйнівних процесів, особливо у країнах колишнього СРСР продовжує стрімко скорочуватися. При збереженні тенденцій зниження фінансування науки та підтримки діяльності вчених, зокрема Україна ризикує перейти вже в найближчому майбутньому з розряду виробників і експортерів наукового знання в розряд його споживачів і імпортерів, повністю залежних від розвинених країн світу.

Загрози інженерно-технологічного забезпечення суспільства. Сучасні розвинуті країни, стаючи все більш технологічно розвиненими, залежать від світової технології і комплек-

туючих ринків не менше, а навіть більше, аніж вчора. Така обставина вже породжує нові типи загроз національній безпеці для країн, технологічно залежних у цьому відношенні від США. Так, зокрема, Міністерство закордонних справ Німеччини й Бундесвер (армія Німеччини) з міркувань безпеки відмовилися від використання програмного забезпечення корпорації Microsoft. На думку експертів, особливості програмного коду ряду продуктів цієї компанії дозволяють американським спецслужбам проникати в мережі німецьких відомств.

У той же час, США сьогодні і самі потенційно залежні від інтелектуального потенціалу, вироблюваного в інших країнах. Зокрема, число американських учених і інженерів, що народилися і здобули освіту за межами США, стрімко зростає. 45% інженерів у США володіють дипломами, виданими іноземними вищими навчальними закладами. При цьому, рівень наукових знань серед жителів самих США невисокий [22].

Загрози ідеологічного (морально-політичного) забезпечення суспільства. Цього роду інформація виробляється й розповсюджується в основному за допомогою електронних ЗМІ і особливо телебаченням. Дослідження показують, що «телевізійний потік» у світі рухається сьогодні «по вулиці з одностороннім рухом». Основний потік телематеріалів прямує з крупних промислово розвинених країн Заходу (США, Англія, Франція, ФРН) в менш розвинені країни. Одні тільки США щорічно продають телевізійним організаціям інших країн телематеріалів на 100–200 тис. годин мовлення. Закупівлі телепрограм з-за кордону ведуться більшістю країн, але частка матеріалів, що імпортуються, в їх віщанні різна – від одного до ста відсотків. Найчастіше причина такої диспропорції криється в ступені економічного розвитку країни: чим багатша країна, тим вищий ступінь її забезпечення власною телепродукцією, і навпаки.

Загрози культурно-мистецького (розважального, освітнього і виховного) забезпечення суспільства. З появою нових технічних засобів виробництва інформаційно-розважальної продукції домінування розвинутих світових країн (особливо США) на цьому ринку ще більш посилюється. Зокрема, сьогодні обсяги продажів американських відеоігор перевищують вже обсяги продажів голлівудських фільмів.

Викладене вище дозволяє зробити **висновок**, що, безпека є сукупністю умов і чинників, що забезпечують нормальне функціонування і розвиток будь-якої системи. Інформаційна безпека виступає як заперечення (і подолання) інформаційної небезпеки, що виявляється в будь-яких масштабах. Небезпеки і загрози інформаційній безпеці визначають зміст діяльності з її забезпечення. Забезпечення інформаційної безпеки є не тільки захист від небезпек і загроз в інфосфері суспільства, але й припускає такий позитивний розвиток інформаційної реальності, який не породжував би негативних ефектів процесу інформатизації. Об'єктами забезпечення інформаційної безпеки в системі національної безпеки є особистість, суспільство й держава і їх інтереси в інфосфері. Основним же суб'єктом забезпечення інформаційної безпеки є держава.

Проблема безпеки має яскраво виражений інформаційний аспект. Усі складові інформаційної безпеки є певід'ємними і системотворчими в інших видах безпеки. Таким чином, можна констатувати, що інформаційна безпека пронизує всю решту видів безпеки і її забезпечення є пріоритетним завданням. На сучасному етапі розвитку суспільства без забезпечення інформаційної безпеки практично неможливо забезпечити ніякий інший вид безпеки і національну безпеку країни в цілому.

Література

1. Барсуков В. С. Электромагнитный терроризм: защита и противодействие / Барсуков В. С. [Електронний ресурс]. – Режим доступу : http:// ess.ru/publications/6_2003/barsukov/barsukov.htm.

2. Голубев В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами / Голубев В. О. – Запоріжжя : Просвіта, 2003. 250 с.

3. Дзлиев М. И. Проблемы безопасности: теоретико-методологические аспекты / Дзлиев М. И., Романович А. Л., Урсул А. Д. М., 2001. 240 с.

4. Дзьобань О. П. Соціокультурні аспекти інформаційної безпеки / Дзьобань О. П., Панфілов О. Ю. // Зовнішня торгівля: економіка, фінанси, право. Науковий журнал. 2013. № 2. С. 171-176.

5. Дзьобань О. П. Інформаційне насильство та безпека: світоглядно-правові аспекти : монографія / Дзьобань О. П., Пилипчук В. Г. / За заг. ред. проф. В. Г. Пилипчука. Харків : Майдан, 2011. 244 с.

6. Екологічна безпека територій: колект : монографія / О. М. Адаменко та ін.; за ред. проф., О. М. Адаменка та д-ра техн. наук Я. О. Адаменка. Івано-Франківськ : Супрун В. П. [вид.], 2014. 442 с.

7. Екологічна та біологічна безпека основа національної безпеки України : монографія / Волосянко О. В. та ін. Херсон : Грінь Д. С., 2014. 167 с.

8. Кара-Мурза С. Г. Манипуляция сознанием / С. Г. Кара-Мурза. М. : ЭКСМО-Пресс, 2001 340 с.

9. Лопатин В. Н. Информационная безопасность России: Человек. Общество. Государство. СПб. : Фонд „Университет», 2000. – 278 с.

10. Маслов А. О. Інформаційна економіка: становлення, структура та теоретичне осмислення : монографія / А. О.Маслов. – К. : Аграр Медіа Груп, 2012. – 431 с.

11. Нечитайло Д. А. Джихад в информационном пространстве (киберджихад) / Д. А. Нечитайло [Електронний ресурс]. – Режим доступу : http://antiterror.ru/library/smi/144812970.

12. Новиков В. К. Информационное оружие – оружие современных и будущих войн / В. К. Новиков. – М. : Горячая линия-Телеком, 2011. – 262 с.

13. Соціальні ризики та соціальна безпека в умовах природних і техногенних надзвичайних ситуацій та катастроф / відп. ред. В. В. Дурдинець [та ін.]. – К. : Стилос, 2001. – 496 с.

14. Соціальна безпека: теорія та українська практика / І.Ф.Гнибіденко [та ін.]; ред. І. Ф. Гнибіденко [та ін.]. К. : КНЕУ, 2006. 291 с.; Куценко В. І. http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=EC&P21DBN=EC&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=M=&S21COLORTERMS=0&S21STR=Соціальна безпека в контексті сталого розвитку : монографія / В. І. Куценко, В. П. Удовиченко. – Чернігів: Лозовий В.М., 2011. – 652 с.

15. Супертерроризм: новый вызов нового века ; Под общ. ред. А. В. Федорова. – М. : Права человека, 2002. 240 с.

16. Тоффлер Э. Метаморфозы власти / Тоффлер Э. М. : ООО «Издательство АСТ», 2001. 800 с.

17. Урсул А. Д. Информатизация общества. Введение в социальную информатику / А. Д. Урсул. М. : Наука, 1990. 340 с.

18. Aum Shinri-kyo and Related Controversies [Електронний ресурс]. Режим доступу : http://www.cesnur.org/testi/aumI.htm.

19. Report by the Center for the Study of Terrorism and Irregular Warfare at the Naval Post-graduate School [Електронний ресурс]. Режим доступу : http://www.nps.naw.mil/ctiw/reports.

20. Sirak M. U. S. vulnerable to EMP Attack / M. Sirak // 26 July [Електронний ресурс]. Режим доступу : http://wAv\v.ianes.com/defence/news/idw/.

21. Terrorism: An Introduction [Електронний ресурс]. – Режим доступу : http://www.terrorismanswers.com/terrorism.

22. Washington ProFile (Независимая информация и аналитика из США) [Електронний ресурс]. – Режим доступу : http:// www. washprofile.org/ru/node/3515].

References

1. Barsukov V. S. Elektromagnitnyj terrorizm: zaschita i protivodeystvie. – http:// ess.ru/publications/6_2003/barsukov/barsukov.htm.

2. Holubev V. O. Informatsiina bezpeka: problemy borotby z kiberzlochynamy. Zaporizhzhia : Prosvita, 2003. 250 s.

3. Dzliev M.I. Problemy bezopasnosti: teoretiko-metodologicheskie aspekty / Dzliev M.I., Romanovich A.L., Ursul A.D. M., 2001. 240 s.

4. Dzoban O.P. Sotsiokulturni aspekty informatsiinoi bezpeky / Dzoban O.P., Panfilov O.Yu. // Zovnishnia torhivlia: ekonomika, finansy, pravo. Naukovyi zhurnal. 2013. # 2. S. 171-176.

5. Dzoban O.P. Informatsiine nasylstvo ta bezpeka: svitohliadno-pravovi aspekty: Monohrafiia / Dzoban O.P., Pylypchuk V.H. / Za zah. red. prof. V.H.Pylypchuka. Kharkiv: Maidan, 2011. 244 s.

6. Ekolohichna bezpeka terytorii: kolekt. monohrafiia / O.M.Adamenko ta in.; za red. prof., O.M.Adamenka ta d-ra tekhn. nauk Ya.O.Adamenka. – Ivano-Frankivsk: Suprun V. P. [vyd.], 2014. – 442 s.

7. Ekolohichna ta biolohichna bezpeka – osnova natsionalnoi bezpeky Ukrainy: monohrafiia / Volosianko O.V. ta in. – Kherson: Hrin D.S., 2014. – 167 s.

8. Kara-Murza S.G. Manipulyatsiya soznaniem / S.G. Kara-Murza. – M. : EKSMO-Press, 2001 – 340 s.

9. Lopatin V.N. Informatsionnaya bezopasnost' Rossii: Chelovek. Obschestvo. Gosudarstvo. – SPb.: Fond „Universitet», 2000. – 278 s.

10. Maslov A.O. Informatsiina ekonomika: stanovlennia, struktura ta teoretychne osmyslennia: monohrafiia / A.O.Maslov. – K.: Ahrar Media Hrup, 2012. – 431 s.

11. Nechitaylo D. A. Dzhihad v informatsionnom prostranstve (kiberdzhihad) / D.A. Nechitaylo [Elektronnyi resurs]. – Rezhym dostupu : http://antiterror.ru/library/smi/144812970.

12. Novikov V.K. Informatsionnoe oruzhie – oruzhie sovremennyh i buduschih voyn / V.K.Novikov. – M. : Goryachaya liniya-Telekom, 2011. – 262 s.

13. Sotsialni ryzyky ta sotsialna bezpeka v umovakh pryrodnykh i tekhnohennykh nadzvychainykh sytuatsii ta katastrof / vidp. red. V.V.Durdynets [ta in.]. – K.: Stylos, 2001. – 496 s.

14. Sotsialna bezpeka: teoriia ta ukrainska praktyka / I.F.Hnybidenko [ta in.]; red. I.F.Hnybidenko [ta in.]. K.: KNEU, 2006. 291 s.; Kutsenko V.I. Sotsialna bezpeka v konteksti staloho rozvytku: monohrafiia / V.I.Kutsenko, V.P.Udovychenko. Chernihiv: Lozovyi V.M., 2011. 652 s.

15. Superterrorizm: novyj vyzov novogo veka ; Pod obsch. red. A. V. Fedorova. M. : Prava cheloveka, 2002 240 s.

16. Toffler E. Metamorfozy vlasti / Toffler E. M. : OOO «Izdatel'stvo ACT», 2001. 800 s.

17. Ursul A.D. Informatizatsiya obschestva. Vvedenie v sotsial'nuyu informatiku / A.D. Ursul. M : Nauka, 1990. 340 s.

18. Aum Shinri-kyo and Related Controversies [Elektronnyi resurs]. Rezhym dostupu : http://www.cesnur.org/testi/auml.htm.

19. Report by the Center for the Study of Terrorism and Irregular Warfare at the Naval Post-graduate School [Elektronnyi resurs]. – Rezhym dostupu : http://www.nps,naw.mil/ctiw/reports.

20. Sirak M. U. S. vulnerable to EMP Attack / M. Sirak // 26 July [Elektronnyi resurs]. – Rezhym dostupu : http://wAv\v.ianes.com/defence/news/idw/.

21. Terrorism: An Introduction [Elektronnyi resurs]. – Rezhym dostupu: http://www.terrorismanswers.com/terrorism.

22. Washington ProFile (Nezavysymaia ynformatsyia y analytyka yz SShA) [Elektronnyi resurs]. – Rezhym dostupu : http:// www. washprofile.org/ru/node/3515].

О. П. Дзьобань, А.Ю. Панфилов, Р. А. Чемчикаленко

ИНФОРМАЦИОННЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ В СОЦИОКУЛЬТУРНЫХ ПРОЦЕССАХ

Анотация: *В статье раскрываются информационные аспекты безопасности современного общества и его социокультурных процессов. Показано, что все составляющие информационной безопасности являются неотъемлемыми и системообразующими в других видах безопасности. Констатируется, что информационная безопасность пронизывает все виды безопасности и ее обеспечение является приоритетной задачей. Рассматривается роль информационной безопасности в экономических процессах и процессах обеспечения обороноспособности государства. Освещается роль информационной войны и информационного терроризма в создании информационных угроз в социуме. Обосновывается, что на современном этапе развития общества без обеспечения информационной безопасности практически невозможно обеспечить никакой другой вид безопасности и национальную безопасность страны в целом. Предложено новую типологию основных групп угроз обществу в информационной сфере.*

Ключевые слова: *информационная безопасность общества, социальная безопасность, информационная война, информационный терроризм, угрозы информационной безопасности.*

Dzoban A., Panfilov O., Chemchykalenko R.

INFORMATION SECURITY ASPECTS IN THE SOCIO-CULTURAL PROCESSES INFORMATION SECURITY ISSUES

Annotation: *The article describes the information security aspects of modern society and its social and cultural processes. It is shown that all the components of information security are essential backbone and are in other kinds of security. It is states that information security permeates all kinds of safety and its providing is a priority. The article examines the role of information security in the economic process and the process of defense of the state. It highlights the role of information warfare and information terrorism in the creation of information threats in society. It is proved that at the present stage of development of society it is practically impossible to provide any other kind of security and national security of the country as a whole without information security. It is suggested a new typology of main groups society threats in the information sphere.*

Keywords: *information security of the society, social security, information warfare, information terrorism, threats to information security.*

Стаття надійшла до редакції 23.02.2015 р.