УДК 351.746.1(477)

Л. В. БОРИСОВА,
кандидат юридичних наук, доцент,
доцент кафедри інформаційної безпеки
факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ,

В. В. ТУЛУПОВ,
кандидат технічних наук, доцент,
доцент кафедри інформаційної безпеки
факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ВИЗНАЧАЛЬНИЙ КОМПОНЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Проаналізовано проблеми інформаційної безпеки на міжнародному рівні. Означено загрози інформаційній безпеці в національному інформаційному просторі України. Цілі інформаційної політики визначені пріоритетністю національних інтересів як унеможливлення реалізації загроз для інформації.

Ключові слова: *інформаційна безпека, національна безпека, загрози інформаційної безпеці, національний інформаційний простір, інформаційна політика, міжнародне співробітництво.*

Процеси, що відбуваються в суспільному житті, можна охарактеризувати як посилення ролі та значення інформації і в суспільстві в цілому, і в житті кожної людини зокрема. Інформація отримує реальне матеріально-енергетичне, соціально-економічне, політичне і вартісне вираження. За цих умов одним із першочергових завдань, що постають перед правовою державою, є вирішення суперечності між реально існуючими і зростаючими потребами особистості, суспільства і держави в якісних інформаційних ресурсах, продуктах та послугах і необхідністю забезпечення їх інформаційної безпеки. Політика у сфері інформаційної безпеки спрямована на досягнення такого рівня духовного та інтелектуального потенціалів країн, який є достатнім для розвитку державності і соціального прогресу.

Визнання проблеми інформаційної безпеки на міжнародному рівні обумовлюється такими чинниками глобалізації:

– у більшості розвинутих країн проводяться дослідження і розроблення нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного противника, а в необхідних випадках впливати на них[1];

– кардинально змінилася оцінка доктрини інформаційної безпеки в цілому і позиції більшості країн світу, які усвідомили потенціал інформаційних загроз і необхідність створення відповідного міжнародного механізму для контролю інформаційного протиборства.

Політичні дискусії на Міжнародному семінарі з проблем інформаційної безпеки (Женева, 1999 р.), який відбувся під егідою Інституту ООН з дослідження проблем роззброєння (*UNIDIR – United Nations Institute for Disarmament Research*) за участю департаменту з питань роззброєння Секретаріату ООН та представників понад 50-ти країн світу, підтвердили актуальність проблеми та своєчасність її розгляду в рамках ООН. У визначенні підходів до її вирішення виявилися різні позиції, котрі відповідали стратегічним інтересам учасників дискусії. Позиція

[1] За даними аналітичних центрів США, розроблення такої зброї ведеться в 120-ти країнах світу. Для порівняння: розроблення в галузі ядерної зброї проводяться не більше ніж у 20-ти країнах. У деяких країнах завершено розроблення 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 інформаційної сфери від агресії і несанкціонованого втручання; у 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.

розвинутих країн передбачала визнання проблеми міжнародної інформаційної безпеки як:

– гіпотетичного силового протистояння;

– перенесення концепції міжнародної інформаційної безпеки на регіональний або тематичний рівень;

– виділення з комплексної проблеми міжнародної інформаційної безпеки таких складових, як кримінальні та терористичні міжнародні інформаційні загрози і створення міжнародного механізму контролю подібних інформаційних злочинів.

Позиція країн, які не належать до західної моделі цивілізації, передбачала такі пропозиції:

– встановлення міжнародно-правової норми про заборону застосування засобів впливу на інформаційні ресурси та інформаційний потенціал міжнародного, регіонального та національного призначення;

– створення спеціального Міжнародного суду з інформаційної злочинності;

– спільне розроблення технології глобального захисту від інформаційної агресії.

У Заяві міжнародної зустрічі було проголошено узгодження Програми дій щодо запобігання інформаційним війнам та обмеження гонки інформаційних озброєнь.

Женевська зустріч виявила стратегічну проблему міжнародної інформаційної безпеки – проблему домінування в глобальній інформаційній сфері із застосуванням інформаційних озброєнь, тобто прагнення до контролю значних територій та соціумів, проблему інформаційного дисбалансу сил міжнародного світопорядку.

Концепція міжнародної інформаційної безпеки визначає критичні структури, які насамперед зазнають впливу в умовах інформаційного протиборства. Найбільш вразливими вважаються політична, суспільна, економічна, військова, науково-технологічна, духовна сфери життєдіяльності суспільства, а саме:

– 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;

– для економічної сфери критичними вважаються системи загальноекономічного аналізу та прогнозування економічного розвитку, структури прийняття рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, інфраструктури банківських мереж і систем, системи управління в критично важливих для функціонування держави структурах (енергетика, транспортні комунікації, телекомунікаційні та інформаційні мережі);

– у військовій сфері вразливими в умовах інформаційного протиборства вважаються інформаційні ресурси збройних сил, військово-промисловий комплекс, системи управління військами, системи контролю і постійного спостереження, канали надходження інформації стратегічного, оперативного, розвідувального характеру;

– глобальними загрозами в науково-технологічній сфері є феномен транскордонного переміщення інтелектуальних ресурсів, тобто вивезення інформації унікального науково-технологічного характеру на біологічних носіях до міжнародних систем спостереження, аналізу і прогнозування тенденцій науково-технологічного розвитку в різних країнах з метою доступу до конфіденційних баз і банків даних; критичними для безпеки у сфері науки і технологій є структури накопичення науково-технічної інформації, інструкції та структури фундаментальних і прикладних досліджень, об'єкти інтелектуальної власності, ноу-хау;

– суспільна сфера є найбільш вразливою для інформаційних впливів, оскільки включає системи формування громадської думки, структури засобів масової комунікації, 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;

– становище в духовній сфері стає критичним в умовах конфесійного протистояння, релігійного фанатизму, трансформації духовних ідеалів та морально-етичних цінностей. Так, проявом критичності ситуації в духовній сфері (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 внесені до глобальної культурної спадщини і перебувають під охороною ЮНЕСКО.

Загрози інформаційній безпеці реалізуються через порушення інфраструктури, вільного обігу інформації, неправомірні дії щодо інформації, через невідповідність інформаційної політики, засобів інформування громадськості. Відповідно до критичних сфер міжнародного співробітництва класифікуються *загрози для інформаційної безпеки.* Існують різні типології загроз, але шляхом узагальнення, можна виділити такі види загроз:

– інформаційно-технологічні;
– інформаційно-комунікаційні;
– інформаційно-психологічні.

Такі загрози посилюють негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності.

Під *національним інформаційним простором* розуміють усю сукупність інформаційних потоків як національного походження, так і іноземних, що доступні на території держави.

Основними *цілями інформаційної політики України* є забезпечення:

– захисту інформаційного суверенітету держави, особливо захисту національного інформаційного простору з інформаційним ресурсом і системи формування масової суспільної свідомості;

– рівня інформаційної достатності для прийняття рішень державними органами, підприємствами і громадянами;

– реалізації конституційних прав і свобод громадян, суспільства і держави.

Цілі інформаційної політики визначені в Законі України «Про Національну програму інформатизації» від 4 лютого 1998 р. № 74/98-ВР та спрямованих на його реалізацію указах Президента України «Про рішення Ради національної безпеки і оборони України від 17 червня 1997 р. «Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин» від 21 липня 1997 р. № 663/97, «Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади» від 14 липня 2000 р. № 887/2000, «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 р. № 928/2000, «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р. «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» від 6 грудня 2001 р. № 1193/2001; дорученнях Президента України від 12 квітня 2000 р., 5 грудня 2000 р. та 25 квітня 2001 р. щодо створення та забезпечення функціонування національного каналу супутникового іномовлення.

Витік інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері.

У зв'язку з рішенням Ради національної безпеки і оборони України «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» від 21 березня 2008 р., введеним у дію Указом Президента України від 23 квітня 2008 р. № 377/2008, було затверджено Доктрину інформаційної безпеки України (Указ Президента України від 8 липня 2009 р. № 514/2009). У Доктрині наголошено, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

В інформаційній сфері України вирізняються такі життєво важливі інтереси:

1) особи:

– забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

– недопущення несанкціонованого втручання у зміст, процеси оброблення, передання та використання персональних даних;

– захищеність від негативного інформаційно-психологічного впливу;

2) суспільства:

– збереження і примноження духовних, культурних і моральних цінностей українського народу;

– забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди;

– формування і розвиток демократичних інститутів громадянського суспільства;

3) держави:

– недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері;

– побудова та розвиток інформаційного суспільства;

– забезпечення економічного та науково-технологічного розвитку України;

– формування позитивного іміджу України;

– інтеграція України у світовий інформаційний простір.

Діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства і людини за такими трьома головними напрямами:

1) інформаційно-психологічний напрям;

2) технологічний розвиток;

3) захист інформації.

Доктрина інформаційної безпеки України спрямована на забезпечення необхідного рівня інформаційної безпеки України в конкретних умовах даного історичного періоду і є основою для формування державної політики у сфері інформаційної безпеки України.

Державна політика визначається пріоритетністю національних інтересів і має на меті унеможливлення реалізації загроз для інформації.

Метою інформаційної політики держави має бути створення умов для:

– побудови в державі інформаційного суспільства як органічного сегмента глобального інформаційного співтовариства;

– забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури;

– впровадження новітніх інформаційних технологій;

– захисту національних моральних і культурних цінностей;

– забезпечення конституційних прав на вільний доступ до інформації.

Список використаної літератури

1. Доктрина інформаційної безпеки України [Електронний ресурс] : затв. указом Президента України від 8 лип. 2009 р. № 14/2009. – Режим доступу: http://zakon.rada.gov.ua/laws/show/514/2009.

2. Стратегія національної безпеки України «Україна у світі, що змінюється» [Електронний ресурс] : затв. указом Президента України від 12 лют. 2007 р. № 105. – Режим доступу: http://zakon.rada.gov.ua/laws/show/389/2012. – У ред. від 8 черв. 2012 р. № 389/2012.

Надійшла до редколегії 11.03.2013

БОРИСОВА Л. В., ТУЛУПОВ В. В. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОПРЕДЕЛЯЮЩИЙ КОМПОНЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ УКРАИНЫ

Проанализованы проблемы информационной безопасности на международном уровне. Определены угрозы информационной безопасности в национальном информационном пространстве Украины. Цели информационной политики обусловлены приоритетностью национальных интересов как невозможность реализации угроз для информации.

Ключевые слова: *информационная безопасность, национальная безопасность, угрозы информационной безопасности, национальное информационное пространство, информационная политика, международное сотрудничество.*

BORISOVA L., TULUPOV V. INFORMATIONAL SECURITY AS THE KEY FACTOR OF THE NATIONAL SECURITY OF UKRAINE

The problems of informational security on international level are analyzed. The threats to informational security of Ukraine are defined. Also the goals of the informational policy as the priority of the national interests to disable threats to information are determined.

Keywords: *information security, nation security, information security threats, nation information space, information policy, international cooperation.*