УДК 35
doi 10.33287/102019

ПАНЧЕНКО Олег Анатолійович
д-р мед. наук, проф., директор Державного закладу «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України»
ORCID: 0000-0001-9673-6685

ІНФОРМАЦІЙНА БЕЗПЕКА В КОНТЕКСТІ ВИКЛИКІВ І ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

Аналізуються сучасні проблеми інформаційної безпеки в складі національної безпеки держави. Визначаються причини, що зумовлюють незадовільний стан у сфері забезпечення інформаційної безпеки. Особлива увага приділяється правовим основам забезпечення інформаційної безпеки та перспективам удосконалення законодавства, проблемам регулювання відносин у цій сфері. Успішний розвиток України як суверенної держави неможливий без забезпечення її національної безпеки. Інформаційна безпека суспільства і держави визначається мірою їх захищеності, а отже, стійкістю основних сфер життєдіяльності до небезпечних дестабілізуючих, деструктивних інформаційних дій, які утискають інтереси країни.

Ключові слова: інформація, безпека, інформаційна безпека, національна безпека, національні інтереси, інформаційна сфера, національна безпека України.

Постановка проблеми. У сучасному світі роль інформаційної сфери життя суспільства, яка розглядається як сукупність інформації, інформаційної інфраструктури, суб'єктів інформаційних правовідносин та системи регулювання суспільних відносин, що виникають при цьому, постійно зростає. Інформаційна сфера істотно впливає на стан політичної, економічної, оборонної та інших складників безпеки держави. Тобто національна безпека залежить від забезпечення інформаційної безпеки, причому з розвитком інформаційних технологій ця взаємозалежність буде тільки зростати та набувати більшого значення для держави та суспільства загалом. Так, у ст. 17 Конституції України зазначено, що інформаційна безпека є найважливішою функцією держави, справою всього українського народу [4].

Аналіз останніх досліджень і публікацій. Проблемами дослідження у сфері інформаційної безпеки займалися такі науковці, як: В. Гурковський, А. Герасимова, А. Баранов, А. Губенков, Б. Кормич, А. Манойло, А. Позднякова, Г. Почепцов та ін. У своїх працях науковці розглядають проблеми безпеки шляхом комплексного підходу до світового та вітчизняного досвіду її забезпечення, надають рекомендації щодо зміцнення безпеки країни.

Б. Кормич визначає інформаційну безпеку як стан захищеності параметрів інформаційних процесів, відносин і норм, встановлених законодавством. Це забезпечує необхідні умови існування суспільства, держави, людини як суб'єктів таких процесів та відносин [5]. В. Лопатін стверджує, що інформаційна безпека є станом захищеності життєво важливих інтересів держави, суспільства та особи на збалансованій основі, тобто національних інтересів країни, від внутрішніх і зовнішніх загроз в інформаційній сфері [6].

Український учений О. Баранов визнає інформаційну безпеку як стан захищеності національних інтересів країни в інформаційному середовищі. За таких умов зводиться до мінімуму чи не допускається взагалі заподіяння шкоди державі, суспільству чи особі внаслідок несанкціонованого поширення інформації, її недостовірність, несвоєчасність через негативні наслідки функціонування інформаційних технологій чи негативний інформаційний вплив [1].

Мета статті полягає у визначенні ролі інформаційної безпеки в складі національної безпеки держави та дослідженні законодавчого регулювання в інформаційній сфері України.

Викладення основного матеріалу. З розвитком інформаційних технологій та інформаційного суспільства в умовах глобалізації виникло ціле коло невирішених питань і проблем, істотно змінилася характеристика викликів і загроз цивілізації. Головні цінності, для захисту яких держави прагнуть сформувати ефективні механізми протидії викликам і загрозам, – мир, безпека, права людини і стійкий розвиток держави.

На сьогодні єдиної думки щодо визначення поняття «інформаційна безпека» серед дослідників не існує. Тому в межах окресленого підходу інформаційну безпеку можна інтерпретувати як стан захищеності держави, її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства і держави. Національна безпека держави істотно залежить від забезпечення інформаційної безпеки, та в ході технічного прогресу ця залежність тільки збільшується.

Слід виділити три основні напрями забезпечення інформаційної безпеки:

– захист інформаційних прав і свобод людини і громадянина;

– захист інформаційних ресурсів, у тому числі інформації з обмеженим доступом, від неправомірного доступу;

– захист суспільства від шкідливої і неякісної інформації.

Згідно із Законом України «Про Концепцію Національної програми інформатизації» інформаційна безпека є невід'ємною частиною оборонної, економічної, політичної, а також інших складників національної безпеки [8]. Вона забезпечує захищеність життєво важливих інтересів особи, суспільства і держави від внутрішніх і зовнішніх загроз. Отже, національна безпека залежна від змісту національно-державних інтересів та характеризує стан країни, за якого їй не загрожує небезпека війни або інших посягань на суверенний розвиток.

Національна безпека України – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [9].

Основними компонентами національної безпеки є військова, економічна, соціальна, екологічна, інформаційна безпека. Сама по собі національна безпека являє собою геополітичний аспект безпеки загалом, увесь комплекс питань фізичного виживання держави, захисту і збереження його суверенітету і територіальної цілісності. На сьогодні проблема інформаційної безпеки є дуже важливою, оскільки значно зросла роль збирання, обробки і поширення інформації, зокрема збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації. Інформація відіграє все більшу роль у процесі життєдіяльності людини.

Інформаційна безпека суспільства і держави визначається мірою їх захищеності, а отже, стійкістю основних сфер життєдіяльності до небезпечних дестабілізуючих, деструктивних інформаційних дій, які утискають інтереси країни [7].

Інформаційна безпека особи характеризується захищеністю психіки і свідомості від небезпечних інформаційних дій: маніпулювання, дезінформації, спонукання до самогубства, зневаги і под. Необхідно зазначити, що інформаційні дії небезпечні (чи корисні) не стільки самі по собі, скільки тим, що здатні викликати потужні процеси, управляти ними.

Небезпечні інформаційні дії зазвичай розділяють на два види. Перший пов'язаний з утратою цінної інформації, що або знижує ефективність власної діяльності, або підвищує ефективність діяльності супротивника, конкурента. Якщо об'єктом такої дії є свідомість людей, то йдеться про розголошування

державних таємниць, вербування агентів, застосування спеціальних засобів для підслуховування, детекторів брехні, медикаментозні, хімічні та інші дії на психіку людини. Безпеку від таких загроз забезпечують органи цензури, контррозвідки та інші суб'єкти інформаційної безпеки. Якщо ж джерелом інформації є технічні системи, то йдеться вже про технічну розвідку, або шпигунство (перехоплення телефонних розмов, радіограм, сигналів інших систем комунікації), проникнення в комп'ютерні мережі, банки даних.

Другий вид інформаційної дії пов'язаний з упровадженням негативної інформації, що може не лише призвести до небезпечних помилкових рішень, але і змусити завдати шкоду, навіть привести суспільство до катастрофи. Інформаційну безпеку цього виду повинні забезпечувати спеціальні структури інформаційно-технічної боротьби. Їх завдання – нейтралізувати акції дезінформації, перешкоджати маніпулюванню громадською думкою, ліквідовувати наслідки комп'ютерних атак. Розвиток і впровадження в різні сфери життя суспільства нових інформаційних технологій, як і будь-яких інших науково-технічних досягнень, не лише забезпечують комфортність, але нерідко несуть і небезпеку.

Визначимо найбільш суттєві групи інформаційно-технічних небезпек, обумовлених досягненнями науково-технічного прогресу в умовах глобалізації. Перша група пов'язана з бурхливим розвитком нового класу зброї – інформаційної, здатної ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства. У відносно мирних умовах інформаційно-психологічні технології можуть застосовуватися як спеціальні механізми управління кризами і провокації жорстокості на території супротивника. Друга група інформаційно-технічних небезпек для особи, суспільства й держави – це новий клас соціальних злочинів, що ґрунтуються на використанні сучасних інформаційних технологій (махінації з електронними грошима, комп'ютерне хуліганство та ін.). Питання забезпечення інформаційної безпеки як одного з важливих складників національної безпеки держави особливо гостро постало в контексті появи транснаціональної трансграничної комп'ютерної злочинності і кібертероризму. Третя група інформаційних небезпек – використання нових інформаційних технологій з політичною метою.

Можемо зазначити, що на сьогодні відсутня чітко виражена організована система вироблення та реалізації єдиної державної політики у сфері забезпечення інформаційної безпеки, яка визначає пріоритети розвитку єдиного інформаційного простору. Зазначимо причини, що зумовлюють незадовільний стан у сфері забезпечення інформаційної безпеки:

– безсистемний розвиток законодавства, що регулює інформаційну сферу;

– низький рівень правової та інформаційної культури громадян і суспільства загалом;

– незадовільне фінансування діяльності із забезпечення інформаційної безпеки;

– недостатній розвиток інформаційних та комунікаційних технологій у сфері державного управління, неготовність органів державної влади до застосування ефективних технологій управління і організації взаємодії з громадянами і господарюючими суб'єктами;

– недостатній рівень підготовки кадрів у сфері створення і використання інформаційних і комунікаційних технологій.

Основні принципи і зміст діяльності із забезпечення безпеки наведені в Законі України «Про національну безпеку». У цьому законі визначаються та розмежовуються повноваження державних органів у сфері національної безпеки й оборони, створюється основа для інтеграції політики та процедур органів

державної влади, інших державних органів, функції яких стосуються національної безпеки й оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки й оборони, забезпечуючи в такий спосіб демократичний цивільний контроль за органами та формуваннями сектору безпеки й оборони [9].

Основними принципами забезпечення безпеки є: дотримання і захист прав і свобод людини і громадянина; законність; системність і комплексність застосування публічними органами влади політичних, організаційних, соціально-економічних, інформаційних, правових та інших заходів забезпечення безпеки; пріоритет запобіжних заходів для забезпечення безпеки; взаємодія органів державної влади з громадськими об'єднаннями, міжнародними організаціями і громадянами для забезпечення безпеки.

Діяльність держави щодо забезпечення безпеки включає:

– прогнозування, виявлення, аналіз і оцінювання загроз безпеки;

– визначення основних напрямів державної політики і стратегічне планування у сфері забезпечення безпеки;

– правове регулювання у сфері забезпечення безпеки;

– розробку і застосування комплексу оперативних і довготривалих заходів з виявлення, попередження й усунення загроз безпеки, локалізації і нейтралізації наслідків їх прояву;

– застосування спеціальних економічних заходів для забезпечення безпеки;

– розробку, виробництво і впровадження сучасного вигляду озброєння, військової і спеціальної техніки, а також техніки подвійного й цивільного призначення для забезпечення безпеки;

– організацію наукової діяльності у сфері забезпечення безпеки;

– координацію діяльності регіональних органів державної влади, органів державної влади суб'єктів України, органів місцевого самоврядування у сфері забезпечення безпеки;

– фінансування витрат на забезпечення безпеки, контроль за цільовим витрачанням виділених засобів;

– міжнародну співпрацю у сфері забезпечення безпеки;

– здійснення інших заходів у сфері забезпечення безпеки відповідно до законодавства України.

Так, у Законі України «Про Національну програму інформатизації» визначається, що головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави [10].

Таким чином, з вищезазначеного можна зробити висновок, що категорія «безпека» розглядається як поняття, що відображає стан об'єкта в системі його зв'язків з точки зору здатності до самовиживання в умовах внутрішніх та зовнішніх загроз, а також в умовах дій непередбачених та тяжко прогнозованих факторів. Національна безпека України складається із сукупності складників, які повинні забезпечувати збалансовані інтереси особи, суспільства і держави. До цих складників належить безпека в міжнародній економічній, військовій, внутрішньополітичній, інформаційній, соціальній, екологічній та інших сферах. При цьому, як уже зазначалося, одна з ключових ролей у системі забезпечення національної безпеки відводиться економічному та інформаційному складникам.

Базовим документом, що визначає зміст національних інтересів України в інформаційній сфері, є Доктрина інформаційної безпеки України [11]. Правовою основою доктрини є Конституція України [7], закони України, Стратегія

національної безпеки України, затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України"» [12], а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Стратегія національної безпеки України є документом, обов'язковим для виконання, і основою для розробки конкретних програм згідно з державною політикою національної безпеки [11].

У доктрині інформаційної безпеки закріплені актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері:

– здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізація суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

– інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

– неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіакультури суспільства;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [11].

Висновки. Таким чином, можемо зробити висновок, що національна безпека нерозривно пов'язана з діяльністю держави. Тільки вона може, спираючись на свій апарат, владні органи, діяльність яких жорстко обмежена і підкріплена відповідними правовими актами, забезпечити спокій громадян, створити сприятливі умови для їх життя і діяльності. Ніякі інші соціальні сили не зможуть виконати це завдання. Забезпечення власної безпеки та своїх громадян є одним з основних завдань будь-якої держави. Успішний розвиток України як суверенної держави неможливий без забезпечення її національної інформаційної безпеки.

У світі розвитку інформатизації та глобалізації роль інформаційної безпеки особи, суспільства, держави збільшується, а її забезпечення повинне зайняти належне місце в політиці держави. Зазначимо основні завдання щодо забезпечення інформаційної безпеки як складника національної безпеки держави, які вимагають вирішення:

1. Необхідність нормативно-правового регулювання щодо протидії використання інформаційних технологій, які загрожують інтересам держави.

2. Необхідність створення економічних передумов для розвитку національних інформаційних ресурсів та інфраструктури, впровадження новітніх технологій в інформаційну сферу.

3. Необхідність удосконалення виробництва вітчизняних інформаційних технологій, що розробляються, впровадження вітчизняних розробок, підвищення

ефективності наукових досліджень та якості освіти у сфері інформаційних технологій.

Інформація стала одним із чинників, здатних призвести до великомасштабних аварій, військових конфліктів і дезорганізації державного управління. І чим вищий рівень інтелектуалізації та інформатизації суспільства, тим надійніша його інформаційна безпека. Отже, Україні необхідно приділяти особливу увагу національній інформаційній безпеці, оскільки вона є основою визначення найважливіших напрямів і принципів державної політики країни, життєво важливих інтересів особи, держави й суспільства.

Список бібліографічних посилань

1. Баранов А. Информационный суверенитет или информационная безопасность? *Національна безпека і оборона*. 2001. № 1(13). С. 70 – 76.

2. Губенков А. А., Байбурин В. Б. Информационная безопасность. Москва: Новый издат. дом, 2005. 128 с.

3. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: автореф. дис. … канд. юрид. наук: 25.00.02. Київ, 2004. 20 с.

4. Конституція України від 28 черв. 1996 р. № 254к/96-ВР. Київ: Норма права, 2020. 80 с.

5. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юрид. літ., 2003. 472 с.

6. Лопатин В. Н. Информационная безопасность России: Человек. Общество. Государство. Санкт-Петербург: Фонд «Университет», 2000. 428 с.

7. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Гельветика, 2017. 168 с.

8. Про Концепцію Національної програми інформатизації: Закон України від 4 лют. 1998 р. № 75/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80.

9. Про національну безпеку України: Закон України від 21 черв. 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/ laws/show/2469-19.

10. Про Національну програму інформатизації: Закон України від 4 лют. 1998 р. № 74/98-ВР. URL: https://zakon.rada.gov.ua/ laws/show/74/98-%D0%B2%D1%80.

11. Про рішення Ради національної безпеки і оборони України від 29 груд. 2016 р. «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лют. 2017 р. № 47/2017. URL: https://www.president.gov.ua/ documents/472017-21374.

12. Про рішення Ради національної безпеки і оборони України від 6 трав. 2015 р. «Про Стратегію національної безпеки України»: Указ Президента України від 26 трав. 2015 р. № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015.

List of references

1. Baranov A. Informatsionnyiy suverenitet ili informatsionnaya bezopasnost? *Natsionalna bezpeka i oborona.* 2001. № 1(13). P. 70 – 76 [in Russian].

2. Gubenkov A. A., Bayburin V. B. Informatsionnaya bezopasnost. Moskva: Novyiy izdat. dom, 2005. 128 p. [in Russian].

3. Hurkovskyi V. I. Orhanizatsiino-pravovi pytannia vzaiemodii orhaniv derzhavnoi vlady u sferi natsionalnoi informatsiinoi bezpeky: avtoref. dys. … kand. yuryd. nauk: 25.00.02. Kyiv, 2004. 20 p. [in Ukrainian].

4. Konstytutsiia Ukrainy vid 28 cherv.1996 r. № 254k/96-VR. Kyiv: Norma prava, 2020. 80 p. [in Ukrainian].

5. Kormych B. A. Orhanizatsiino-pravovi zasady polityky informatsiinoi bezpeky Ukrainy: monohrafiia. Odesa: Yuryd. lit., 2003. 472 p. [in Ukrainian].

6. Lopatin V. N. Informatsionnaya bezopasnost Rossii: Chelovek. Obschestvo. Gosudarstvo. Sankt-Peterburg: Fond «Universitet», 2000. 428 p. [in Russian].

7. Nashynets-Naumova A. Yu. Informatsiina bezpeka: pytannia pravovoho rehuliuvannia: monohrafiia. Kyiv: Helvetyka, 2017. 168 p. [in Ukrainian].

8. Pro Kontseptsiiu Natsionalnoi prohramy informatyzatsii: Zakon Ukrainy vid 4 liut. 1998 r. № 75/98-VR. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80 [in Ukrainian].

9. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21 cherv. 2018 r. № 2469-VIII. URL: https://zakon.rada.gov.ua/ laws/show/2469-19 [in Ukrainian].

10. Pro Natsionalnu prohramu informatyzatsii: Zakon Ukrainy vid 4 liut. 1998 r. № 74/98-VR. URL: https://zakon.rada.gov.ua/ laws/show/74/98-%D0%B2%D1%80 [in Ukrainian].

11. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrud. 2016 r. «Pro Doktrynu informatsiinoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 25 liut. 2017 r. № 47/ 2017. URL: https://www.president.gov.ua/ documents/472017-21374 [in Ukrainian].

12. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 trav. 2015 r. «Pro Stratehiiu natsionalnoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 26 trav. 2015 r. № 287/ 2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015 [in Ukrainian].

PANCHENKO Oleh
Doctor of Medicine, Professor,
Director of State Institution «Scientific and Practical Medical Rehabilitation and Diagnostic Center of the Ministry of Health of Ukraine»

INFORMATIONAL SECURITY IN THE CONTEXT OF CHALLENGES END THREATS OF NATIONAL SECURITY

The article analyzes the current problems of information security as a part of the national security of the state. The author identifies the reasons for the unsatisfactory situation in the field of information security. Particular attention is paid to the legal framework for information security and prospects for improving legislation, the problems of regulating relations in this area. Successful development and the very existence of Ukraine as a sovereign state is impossible without ensuring its national security. The society's and the state's information security is determined by the degree of their protection and, consequently, the stability of the main areas of life concerning dangerous, destabilizing, destructive, infringing the interests of the country information actions at both implementation, and retrieval.

The state information policy, as activity of system of public authorities and administration in the information-psychological area occupies the central place in the system of regulation of both social and political relations in the modern information society. The transparency of the state information policy is the basis for ensuring the country's socio-psychological stability and successful economic development. The practice of information and psychological influence is more and more developing in the modern world. The terms «informational» and «psychological» wars are widely used by politicians and political scientists, and are increasingly appearing in the context of the country's information security issues.

The purpose of this article is to determine the role of information security in the national security of the state and to study the legislative regulation in the information area of Ukraine.

A radical change in the state's approach to solving this problem should become one of the priorities in ensuring national security.

Key words: information, security, information security, national security, national interests, information area, national security of Ukraine.

Надійшла до редколегії 30.04.20