УДК 354 (477)

А. В. Турчак,
аспірант, Інститут підготовки кадрів державної служби зайнятості України
ORCID ID: 0000-0001-5646-5833

DOI: 10.32702/2306-6814.2019.11.123

ОСНОВНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

A. Turchak,
Postgraduate Student of the Institute of Personnel Training of the State Employment Service of Ukraine

BASIC BASES OF THE STATE POLICY OF PROVIDING INFORMATION SECURITY IN UKRAINE

З'ясовано основні засади державної політики забезпечення інформаційної безпеки в Україні. Визначено, що інформаційну безпеку підтримують, проводячи виважену та збалансовану державну політику в інформаційній галузі. Виявлено, що нині інформаційна безпека в контексті глобалізаційних процесів та міжнародної інтеграції стає особливо важливою. Доведено, що нині інформаційна безпека в контексті глобалізаційних процесів та міжнародної інтеграції стає особливо важливою. Держави, що мають потужний потенціал в інформаційному середовищі, можуть впливати на держави, в яких інформаційний простір та кіберпростір є незахищеними. Упродовж останніх трьох років Україна провела в межах інформаційного простору, Інтернету та кіберпростору більшу кількість заходів по забезпеченню інформаційної безпеки, ніж за весь попередній період незалежності. Законодавчу базу стосовно інформаційної сфери в нашій державі можна вважати однією з кращих, однак завдяки комплексному вивченню маємо можливість побачити моменти, в яких розвинуті демократичні країни значно попереду і які заважають інтеграції до світового інформаційного простору.

The basic principles of the state policy of ensuring information security in Ukraine are elucidated. It is determined that information security is supported by conducting a balanced and balanced state policy in the information sphere. Taking into account that the policy aimed at information security is a complex social phenomenon and combines in particular components of internal and foreign political, economic, technological, military character, a comprehensive approach is required in view of administrative law during formation, because it is precisely the question of state policy, that is, certain power relations. Currently, the information sphere is the role of the integrative basis of social life, and high-quality information security is considered the conceptual basis for its further evolution. Under such circumstances, the emphasis is greatly shifted to the formation of a well-balanced state information policy, underlying the basis of which would be the systematic research of phenomena in the information sphere, the leading position among which belongs to information security. It is determined that information security in the context of globalization processes and international integration is becoming especially important today. States with a strong potential in the information environment can have an impact on states in which the information space and cyberspace are vulnerable. Over the past three years, Ukraine has provided more information security measures than the entire previous period of independence within the information space, the Internet and cyberspace. It is proved that information security in the context of globalization processes and international integration is becoming especially important today. States with a strong potential in the information environment can have an impact on states in which the information space and cyberspace are vulnerable. Over the past three years, Ukraine has provided more information security measures than the entire previous period of independence within the information space, the Internet

and cyberspace. The legislative framework for the information sphere in our state can be considered one of the best, but due to the comprehensive study we have the opportunity to see the moments in which developed democratic countries are far ahead and which hinder integration into the world information space.

Ключові слова: державна політика, інформація, інформаційна безпека, національна безпека, суспільство.
Key words: state policy, information, information security, national security, society.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Дбаючи про захист інформаційних інтересів, будь-яка країна має приділити значну увагу своїй інформаційній безпеці. Зокрема це потрібно, щоб зміцнити українську державність. Відбувається формування української збалансованої державної інформаційної політики в якості складової частини соціально-економічного розвитку країни, керуючись пріоритетами, продиктованими національними інтересами та загрозами національній безпеці. З погляду права, в її основі лежать засади, на яких базується правова демократична держава, а впровадити її можна, розробляючи та реалізуючи відповідні національні доктрини, стратегії, концепції та програми відповідно до чинного законодавства.

Російська Федерація, застосовуючи притаманні гібридній війні технології проти нашої держави, стимулювала перетворення інформаційної сфери на головне поле протистояння. Саме Україна стала об'єктом використаних Російською Федерацією найновіших інформаційних технологій з метою вплинути на свідомість українців, розпалити національну, релігійну ворожнечу, пропагувати агресивну війну, пасильницьки змінити конституційний лад або порушити суверенітет і територіальну цілісність України. У зв'язку з комплексним характером, що мають актуальні загрози національній інформаційній безпеці, варто визначити інноваційні підходи у формуванні захисних систем та розвиткові інформаційного середовища в обставинах, продиктованих глобалізацією та вільним обігом даних.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ, В ЯКИХ ЗАПОЧАТКОВАНО РОЗВ'ЯЗАННЯ ДАНОЇ ПРОБЛЕМИ І НА ЯКІ СПИРАЄТЬСЯ АВТОР, ВИДІЛЕННЯ НЕ ВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ ОЗНАЧЕНА СТАТТЯ

Питанням інформаційної безпеки присвячували свої дослідження такі провідні науковці: Гурковський В.І., Козубський В.О., Макаренко Є.А., Фомін В.О. та інші. Проте. Станом на сьогодні є актуальним дослідження основних засад державної політики забезпечення інформаційної безпеки в Україні, що зумовило вибір теми даної статті.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою статті є з'ясування основних засад державної політики забезпечення інформаційної безпеки в Україні.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ З ПОВНИМ ОБГРУНТУВАННЯМ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

Інформаційну безпеку підтримують, проводячи виважену та збалансовану державну політику в інформаційній галузі. Беручи до уваги те, що націлена на інформаційну безпеку політика є комплексним суспільним явищем і поєднує зокрема складові внутрішньо- і зовнішньополітичного, економічного, технологічного, військового характеру, необхідний комплексний підхід з огляду на адміністративно-правові норми під час формування, адже мова йде саме про державну політику, тобто певні владні відносини. Нині інформаційній сфері належить роль інтегруючої основи суспільного життя, а якісна інформаційна безпека вважається концептуальною засадою його подальшої еволюції. За таких обставин акцент сильно зміщується на те, щоб формувалася виважена державна інформаційна політика, у фундаменті якої лежали б системні наукові дослідження явищ в інформаційній сфері, провідна позиція серед яких належить інформаційній безпеці.

Останніми роками все більше актуалізуються питання підтримки інформаційної безпеки. Владні структури усвідомлюють проблеми і рівень складності задач, пов'язаних із забезпеченням інформаційної безпеки в Україні. Наразі варто комплексно дослідити стан забезпечення інформаційної безпеки та знайти імовірні способи, щоб удосконалити її.

Здійснюється намагання виокремити площини, поза якими ці чинники стають загрозою для життєдіяльності суспільства, і дібрати підходящий інструментарій і формат з метою адекватного прийняття рішень та реагування на ряд існуючих і потенційних загроз національній безпеці через реальну ситуацію в державній інформаційній політиці України.

Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є [5]:

— 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 дестабілізацію 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 медіа-культури суспільства;

— поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Оскільки населенню все більше потрібна інформація, державою повинні бути прораховані кожні виклик та проблема, швидко проведена модернізація в стратегічно важливих частинах держсектору. Отже, сучасне суспільство в умовах модернізації потребує перегляду існуючих економічних, політичних, соціально-культурних концепцій розвитку та інформування суспільства про такі перетворення.

Водночас розвитку інформаційних технологій, необхідного для того, щоб накопичити і ефективно використовувати інформаційні ресурси, надається значення стратегічного чинника у забезпеченні національної безпеки, принципового для політики держави в інформаційній сфері. Керівництво держави усвідомлює, що політична система та суспільна демократизація не будуть ефективно розвиватися через інформаційні загрози.

Зараз, на жаль, для України поняття "інформаційної безпеки", "інформаційної війни", "кібертероризму" лише набирають актуальності. Тож охарактеризуємо ці явища докладніше.

Ще в 2005 році Козубський В.О. звернув увагу на проблеми та загрози стабільності в кримському регіоні, які пов'язані з недосконалістю інформаційної політики. Автор наголошує, що тривала аналітична діяльність у сфері кримського сегменту національного інформаційного простору усе більше переконує не тільки в тому, що кардинальні рішення просто відсутні, але й у тому, що конструктивний шлях стабілізації автономії лежить насамперед у послідовній і кропіткій роботі з суспільною думкою" [3, с. 4].

Справді, державну інформаційну політику нашої країни в Криму можна охарактеризувати як слабку. Російська інформаційна політика формувала настрої кримського населення сильніше, ніж українська.

Коли в Українській державі почало формуватися інформаційне суспільство, а власне Україна увійшла у світовий інформаційний простір, вона постала перед рядом задач, які нагально необхідно вирішити. Особливо актуально для сучасного суспільства — вирішити проблеми, пов'язані з інформаційною безпекою.

У час, коли інформаційна безпека зіштовхується з новими загрозами, державою повинно здійснюватися впровадження і нових методів інформаційного захисту. Новизною дослідницької роботи є те, що буде здійснена систематизація характерних для інформаційного простору загроз, порівняння вже існуючих методів їхньої протидії та надані пропозиції нових ефективних методів боротьби з інформаційними загрозами в межах провадження інформаційної політики держави.

В. Фомін та А. Рось, зауважують, що суть інформаційної безпеки в системі національної безпеки держави полягає в такому: прагненням кожної держави реалізувати та захистити власні національні інтереси, що направлені на формування та накопичення національного інформаційного потенціалу в умовах глобалізації світових інформаційних процесів [6, с. 24]. Зрозуміло, що для розвинутих країн захист свого інформаційного простору є легшим завданням, ніж для менш розвинених. Це завдання потребує не лише значного матеріального забезпечення, але і належного числа кваліфікованих фахівців у цій сфері. Чи є в розвинутих країн зацікавлення в допомозі державам, що мають гірше технологічне забезпечення, з метою зміцнити глобальну міжнародну інформаційну безпеку шляхом впровадження сучасних технологій? Очевидним є те, що власні інтереси будуть пріоритетними для розвинутих світових держав. Вони враховуватимуть стан справ на світовій арені, прораховуватимуть всі здобутки і втрати у разі, якщо нададуть таку допомогу.

Як зауважує Є. Макаренко, проблеми глобальної безпеки посідають особливе місце в структурі міжнародної інформаційної політики, визначають суперечності сучасного етапу міжнародного розвитку, які досягли такого рівня і гостроти, що можуть поставити під загрозу забезпечення світопорядку, реалізацію стратегій становлення глобального інформаційного суспільства, навіть саме існування цивілізації [4, с. 20].

Геополітична позиція нашої країни значною мірою є визначальною для політичного курсу різних політсил, що були при владі в різний час, а з цим і управлінської системи стосовно підтримки інформаційної безпеки. Сьогодні політична система в Україні розвивається в напрямку демократизації соціуму та запровадження цінностей європейського зразка.

Інформаційна безпека України нині має безліч проблем. Серед основних — це захист даних, які можуть бути використані, щоб порушити державну цілісність, або супроти владних інституцій, від роботи яких залежить українське суспільство.

Особливого значення в контексті забезпечення інформаційної безпеки надають кібертероризму. По-

рівняно з традиційним тероризмом цьому різновиду притаманне використання сучасних інформаційно-технологічних інструментів, зловмисне створення інформаційної загрози для життєво-важливих інтересів індивіда і соціуму. У зв'язку з цим застосовують більшу кількість методів вирішення завдань.

2017 року хакерська атака, здійснена комп'ютерним вірусом Petya, сильно пошкодила українську інформаційну інфраструктуру. Через це зазнали збитків багато національних стратегічних об'єктів, комерційних установ та пересічних громадян. Цей напад став можливий внаслідок того, що інформаційні ресурси не мали достатнього рівня захищеності, а правилами кібернетичної безпеки було знехтувано. Атака мала на меті дестабілізувати політичну систему в Україні, створити хаос в інформаційній сфері.

Проведення кібервоєн в Інтернеті породжує низку складних, різнобічних та імовірно дуже небезпечних загроз. Комп'ютерні системи, з'єднані з глобальною мережею, є предметом сильної залежності будь-якого сучасного суспільства, а тому вороги мають більше варіантів для атаки.

У журналі The Economist, зазначається, що "як і в разі контролю над ядерним та звичайним озброєнням, великі країни повинні почати говорити про те, як зменшити загрозу кібервійни, мета — обмежити напади, перш ніж буде занадто пізно [7].

Отже, сьогодні, поряд із землею, морським та повітряним простором своє місце як поле для бойових дій зайняв і кіберпростір.

Наступна проблема в системі забезпечення інформаційної безпеки, яка існує в нашому суспільстві, це проблема доступу до інформації громадськості. Ця проблема певною мірою пов'язана з проблемою захищеності інформаційного простору від несанкціонованих атак та ведення інформаційної війни в площині українського інформаційного простору. Тобто варто відмітити, що в будь-якій державі є секретна інформація, доступ до якої може бути дозволений через багато років, тоді, коли знімається гриф секретності. Це, насамперед, та інформація, розповсюдження, оприлюднення якої може завдати шкоди як державі, так і суспільству. Передусім, як відмічається в монографії "Інформаційна політика України: європейський контекст" (2007), "інформаційна безпека — це завжди балансування між інформаційною відкритістю та закритістю, між прагненнями максимально розширити доступ громадян до невтаємниченої публічної інформації (державної, комерційної, наукової, освітньої, персональної тощо) й максимально захистити інформацію корпоративного і приватного змісту" [2, с. 120].

Необхідно зауважити, що нині українською владою підтримується євроінтеграційний вектор та задекларовано намір підтримувати вільний доступ людей до інформаційних джерел та реалізовувати принцип відкритості ухвалення будь-якого рішення. В обставинах, коли реалізуються демократичні принципи та конституційні права громадянина щодо вільного доступу до інформації, соціально активна частина населення відчула потребу розширити інформаційну взаємодію із владою.

Але зараз, коли відбуваються спроби побудови демократичного, відкритого суспільства, варто взяти до відома посилення ролі явищ інформаційної війни та інформаційного протиборства, а також кібертероризму, що має на меті отримання секретних даних країн, щоб створити в них хаос.

З одного погляду, захист прав і свобод людини, зокрема права на інформацію та права на захист інформації, є невід'ємною частиною громадянських прав у демократичній країні. З іншого — в умовах ведення проти нашої країни інформаційної війни задля захисту індивіда від міжнародних кібертерористичних дій доводиться блокувати деякі веб-сторінки, за допомогою яких може розповсюджуватися інформація, покликана дестабілізувати політичну систему держави. Ці дії мають на меті попередити терористичні акти. Така превентивна діяльність країни зрозуміло викликає сумніви стосовно того, чи зберігаються демократичні принципи.

Наразі в жодній точці світу людині не вдасться почувати себе безпечно — ні в розвинутій країні, ні в тій, що розвивається. В уявленні щодо "безпечних" країн відбулися зміни.

Варто враховувати, що кібертероризм — явище, якому дуже складно протистояти. "Інформаційна зброя", використовувана кібертерористами, є специфічною. Якщо стосовно скорочення решти типів зброї країни періодично ведуть перемовини, то про "інформаційну зброю" домовитися буде непросто, якщо не сказати неможливо. У зв'язку з цим дана сфера є небезпечнішою. Аналітикам не вдається спрогнозувати ступінь влади, яка може опинитися в руках сучасних кібезлочинців, та визначити їхні наступні цілі. Отже, державам, зокрема й Україні, варто бути в готовності захищатися будь-коли.

Національна безпека Української держави в інформаційному просторі перебуває у взаємозв'язку з міжнародною безпекою. У випадку, коли загалом у світі стало небезпечно, окрема держава не може бути безпечною.

Для України є актуальним питання взаємодії органів державної влади щодо гарантування інформаційної безпеки держави. В. Гурковській наголошує, що від органів державної влади очікується вдосконалення не тільки технічного захисту власних систем безпеки комп'ютерних, інформаційних мереж, а й розробки нових підходів та організаційно-правових заходів щодо взаємодії з іншими державними органами, здатними розв'язувати зазначені проблеми на національному рівні [1, с. 3].

Отож, нині інформаційна безпека в контексті глобалізаційних процесів та міжнародної інтеграції стає особливо важливою. Держави, що мають потужний потенціал в інформаційному середовищі, можуть впливати на держави, в яких інформаційний простір та кіберпростір є незахищеними. Продовж останніх трьох років Україна провела в межах інформаційного простору, Інтернету та кіберпростору більшу кількість заходів по забезпеченню інформаційної безпеки, ніж за весь попередній період незалежності.

Законодавчу базу стосовно інформаційної сфери в нашій державі можна вважати однією з кращих, однак завдяки комплексному вивченню маємо можливість побачити моменти, в яких розвинуті демократичні країни значно попереду і які заважають інтеграції до світового інформаційного простору.

Тож влада має усунути низку загроз, які знижують рівень державної інформаційної безпеки: послаблену увагу до проблем, пов'язаних з інформаційною безпекою; недоліки правової бази; застарілий матеріально-технологічний захист мереж; нестачу висококваліфікованих спеціалістів у галузі інформаційного захисту; нестабільні економічні, соціальні та політичні умови в державі тощо.

Вагомі результати можна отримати, налагодивши тісну співпрацю уряду та приватного сектору. Значна робота по забезпеченню того, щоб злочинці і "кіберворіни" не користувалися звичайними комп'ютерними системами, може бути виконана постачальниками Інтернету, які контролюють мережу. Ці надавачі послуг можуть стати відповідальними за локалізацію зараженої комп'ютерної техніки та ідентифікацію нападів. Цих заходів, звісно, недостатньо для очищення інформаційної сфери від злочинних дій чи для того, щоб ліквідувати шпигунство або війни в кібернетичному просторі, але це може трохи підвищити рівень безпеки.

Нейтралізація впливу інформаційних небезпек має бути покладена на державну систему інформаційної безпеки, якої наразі в нашій країні ще немає.

Проаналізувавши досліджувані напрями, в яких здійснюється державна політика забезпечення інформаційної безпеки України, здійснюється комплексний підхід до вирішення проблемних питань в інформаційній безпеці, зауважимо, що формуватися та реалізуватися державна політика у зазначеній галузі має з усвідомленням кожної загрози і небезпеки. Визначення їхніх джерел повинно бути причиною для того, щоб адміністративно-правовим чином окреслити повноваження і функції системи, покликаної організаційно забезпечити інформаційну безпеку та регулювати відносини у межах цієї сфери.

ВИСНОВКИ З ПРОВЕДЕНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ЦЬОМУ НАПРЯМІ

Нині інформаційна безпека в контексті глобалізаційних процесів та міжнародної інтеграції стає особливо важливою. Держави, що мають потужний потенціал в інформаційному середовищі, можуть впливати на держави, в яких інформаційний простір та кіберпростір є незахищеними. Продовж останніх трьох років Україна провела в межах інформаційного простору, Інтернету та кіберпростору більшу кількість заходів по забезпеченню інформаційної безпеки, ніж за весь попередній період незалежності. Законодавчу базу стосовно інформаційної сфери в нашій державі можна вважати однією з кращих, однак завдяки комплексному вивченню маємо можливість побачити моменти, в яких розвинуті демократичні країни значно попереду і які заважають інтеграції до світового інформаційного простору.

Перспективами подальших розвідок у цьому напрямі буде напрацювання напрямів удосконалення державної політики забезпечення інформаційної безпеки в Україні.

Література:

1. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: автореф. дис.... канд. наук з держ. управ.: спец. 25.00.02 / В.І. Гурковський; Нац. акад. держ. управ. при Президентові України. — К., 2004. — 23 с.

2. Інформаційна політика України: європейський контекст: моногр. / Л.В. Губерський, Є.Є. Камінський, Є.А. Макаренко та ін. — К.: Либідь, 2007. — 360 с.

3. Козубський В.О. Інформаційна безпека держави: Кримський регіон: автореф. дис.... канд. політ. наук: спец. 23.00.02 / Валентин Олексійович Козубський; Тавр. нац. універ. ім. В.І. Вернадського. — Сімферополь, 2005. — 19 с.

4. Макаренко Є.А. Міжнародна інформаційна політика: структура, тенденції, перспективи: автореф. дис.... д-ра політ. наук: 23.00.04 / Євгенія Анатоліївна Макаренко; Київський національний ун-т ім. Т. Шевченка. — К., 2002. — 66 с.

5. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України". Указ Президента України від 25.02.2017 №47/2017 [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/47/2017

6. Фомін В.О. Сутність і співвідношення понять "інформаційна безпека", "інформаційна війна" та "інформаційна боротьба" / В.О. Фомін, А.О. Рось // Наука і оборона. — 1999. — № 4. — С. 23—32.

7. Cyberwar [Electronic resource] // The Economist. — 2010. — July 3. — Mode of access: http://www.economi st.com/node/16481504

References:

1. Hurkovs'kyj, V.I. (2004), "Organizational-legal issues of interaction of public authorities in the field of national information security", Ph.D. Thesis, Public Administration, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.

2. Hubers'kyj, L.V. Kamins'kyj, Ye.Ye. and Makarenko, Ye.A. (2007), Informatsijna polityka Ukrainy: ievropejs'kyj kontekst [Information Policy of Ukraine: European Context], Lybid', Kyiv, Ukraine.

3. Kozubs'kyj, V.O. (2005), "Information security of the state: Crimean region", Ph.D. Thesis, Politic, Tavrijs'kyj natsional'nyj universytet im. V. I. Vernads'koho, Simferopol, Ukraine.

4. Makarenko, Ye.A. (2002), "International information policy: structure, trends, perspectives", D.n. Thesis, Political sciences, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.

5. President of Ukraine (2017), Decree "On the Doctrine of Information Security of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/47/2017 (Accessed 20 May 2019).

6. Fomin, V.O. (1999), "The essence and correlation of the concepts of "information security", "information war" and "information struggle", Nauka i oborona, vol. 4, pp. 23-32.

7. The Economist (2010), "Cyberwar", available at: http://www.economi st.com/node/16481504 (Accessed 20 May 2019).

Стаття надійшла до редакції 23.05.2019 р.