DOI 10.31558/2519-2949.2019.3.11
УДК 1.101:32.019.5

ORCID ID: http://orcid.org/0000-0003-0980-7313
Захаренко К. В., Національний педагогічний університет імені М. П. Драгоманова

ОСОБЛИВОСТІ ФОРМУВАННЯ ЕФЕКТИВНОЇ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

Діяльність усіх задіяних у сфері інформаційної безпеки державних структур має бути чітко скоординованою в межах загальних програм і планів, а також визначених функцій. Проаналізовано функціонування усіх задіяних у сфері інформаційної безпеки державних структур та зазначено, що їхня діяльність має бути чітко скоординованою в межах загальних програм і планів, а також визначених функцій. Акцентується увага на тому, що сучасна інформаційна політика України характеризується непослідовністю, нескоординованістю у діяльності різних органів влади, непрозорістю в прийнятті та реалізації політичних рішень. Запропоновано для ефективної реалізації програм у галузі інформаційної безпеки держава повинна надавати необхідні матеріальні ресурси, готувати фахівців, розвивати нормативно-правову базу. З огляду на це в українському законодавстві визначені державні структури, які є суб'єктами національної безпеки. Розкрито пріоритетні напрями розвитку національної інформаційної політики та інформаційної безпеки нашої держави сформульовані в національній доктрині інформаційної безпеки України і закріплені в різних законах.

Для ефективної реалізації програм у галузі інформаційної безпеки держава повинна надавати необхідні матеріальні ресурси, готувати фахівців, розвивати законодавчу базу. З огляду на це в українському законодавстві визначені державні структури, які є суб'єктами національної безпеки. Пріоритетні напрями розвитку національної інформаційної політики та інформаційної безпеки нашої держави сформульовані в національній доктрині інформаційної безпеки України і закріплені в різних законах. Але законодавча база з важливих питань інформаційної безпеки є ще безсистемною, а функції щодо забезпечення інформаційної політики та безпеки держави розпорошені між різними структурами, що не сприяє їх раціональному виконанню. Отож, функції і повноваження державних структур стосовно реалізації інформаційної безпеки мають бути виокремлені достатньо чітко й виразно.

Ключові слова: *людина, політика, інформація, культура, державна політика, державні структури, законодавча база, інформаційна безпека.*

Постановка проблеми. Аналізуючи сутнісні характеристики суб'єкт-об'єктних відносин у системі інформаційної безпеки, варто зосередити увагу на діяльності державних структур інформаційної безпеки та проблемі формування ефективної державної інформаційної політики. Така необхідність обумовлена тим, що саме держава та її інституції створюють певну систему координат для реалізації завдань у сфері інформаційної безпеки для інших суб'єктів, задіяних у цьому процесі.

Розробленість теми в науковій літературі. У політичній науці останнім часом активізувалися дослідження, які вивчають проблематику, що стосується здійснення інформаційної політики. У даному контексті варто відзначити роботи М. Зайцева, Ю. Радковець, О. Левченко, О. Косогова та інших. В свою чергу проблематика формування ефективної державної інформаційної політики, ще потребує окремих спеціалізованих розвідок.

Мета статті полягає в тому, щоб здійснити комплексний аналіз формування ефективної державної інформаційної політики та визначення її проблемних аспектів.

Основні положення. У провідних державах світу, які приділяють значну увагу інформаційній безпеці, діяльність усіх суб'єктів (державних та недержавних) базується на системному підході. Він має наступні ключові ознаки: ієрархічність побудови системи; управління та координація діяльності структурних підрозділів системи на найвищому державному рівні; наявність

спеціально створеного не дорадчого, а керівного органу системи; чітка організація взаємодії між складовими системи. Необхідно зауважити, що загальне керівництво системою інформаційної безпеки здійснюється, як правило, головою виконавчої влади через відповідний робочий орган, який розробляє державну інформаційну політику й координує діяльність її складових елементів, якими є підсистеми інформаційної безпеки визначених державних структур (наприклад, Міністерства оборони, Міністерства внутрішніх справ, інших відомств), котрі, у свою чергу, мають у своєму складі підрозділи виявлення, аналізу та протидії інформаційним загрозам як інформаційно-психологічної, так і кібернетичної спрямованості. Найдосконаліші та найпотужніші системи інформаційної безпеки побудовані й успішно функціонують у США, Великій Британії, Ізраїлі, Китаї та деяких інших державах, які є об'єктами постійного потужного зовнішнього інформаційного впливу [1, с. 39].

Узагальнюючи досвід закордонних країн, можна виокремити наступну ієрархію державних структур (суб'єктів) у сфері інформаційної безпеки. Як правило, очолює дану ієрархію глава держави (або керівник виконавчої влади країни) при якому створюється орган управління з питань інформаційної безпеки, який спирається у своїй діяльності на відповідну структуру у Кабінеті міністрів − департамент (управління) інформаційної безпеки та управління інформаційної безпеки при апараті Ради безпеки. Також голові держави (або керівнику виконавчої влади країни) підпорядковуються відповідні підсистеми інформаційної безпеки міністерств і відомств. Так, у Міністерстві закордонних справ − це орган, що відповідає за інформаційну безпеку. У Міністерстві оборони − це Генеральний штаб з наступними структурними підрозділами: підрозділ захисту та безпеки інформації, підрозділ виявлення, аналізу та протидії інформаційним загрозам, підрозділ інформаційних (кібернетичних) операцій та окремий орган реалізації державної інформаційної політики у сфері оборони, який підпорядковується безпосередньо міністру оборони. У Міністерстві внутрішніх справ − це орган виявлення інформаційної злочинності та центр негайного реагування на комп'ютерні інциденти [1, с. 40].

На нашу думку, до вищенаведеної структури державних суб'єктів інформаційної безпеки, з урахуванням вітчизняної специфіки варто додати відповідні підрозділи у Службі безпеки України, Служби зовнішньої розвідки та інших міністерств та відомств, які беруть участь у реалізації державної інформаційної політики (Міністерство освіти та науки України, Міністерство культури тощо). Відповідно всі державні структури, що задіяні у сфері інформаційної безпеки повинні бути скоординовані, діяти в межах загальних програм та планів, а також уникати дублювання функцій.

Для ефективної реалізації програм у сфері інформаційної безпеки держава повинна надавати необхідні матеріальні ресурси, готувати фахівців відповідного спрямування, використовувати закордонний досвід тощо. В українському законодавстві визначені державні структури, що є суб'єктами національної безпеки, але недостатньо чітко виокремлені їх функції та повноваження у сфері інформаційної безпеки. Так, забезпечення національної безпеки покладається на таких суб'єктів: – Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки і оборони України, які здійснюють загальне керівництво, координацію та контроль за реалізацією заходів у сфері національної безпеки; – міністерства та інші центральні органи виконавчої влади; Національний банк України; суди загальної юрисдикції; прокуратура України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України, на які безпосередньо покладається виконання заходів у сфері національної безпеки [2].

На сьогоднішній день в Україні створений спеціальний державний орган − Міністерство інформації, який буде займатися виключно проблемами вироблення ефективної інформаційної політики та певною мірою інформаційною безпекою держави. Хоча у парламенті та у суспільстві створення даної структури оцінюється неоднозначно. Як підкреслив керівник даного відомства Ю. Стець, за час існування незалежної України не була створена концепція інформаційної політики, тому один з департаментів Міністерства інформації буде опікуватися саме створенням цієї стратегії і її впровадженням. Ще один департамент буде займатися відображенням інформаційних загроз з боку Росії і країн-лобістів РФ. За словами міністра, представники цього департаменту будуть займатися створенням концепції інформаційної безпеки України. Третій департамент має на меті налагодити комунікацію між органами влади з дотримання єдиної позиції, формуванням меседжів, які треба доносити в Україні і в світі. Міністр зауважив, що

на створення цього міністерства його надихнув досвід Великобританії, Франції і США, де такі міністерства існували під час Першої світової війни і відновлені у 1938 році [3]. На думку фахівців, законодавча база з цих важливих питань є не системною, а функції щодо забезпечення інформаційної політики та безпеки держави розпорошені між різними структурами, що відповідно не сприяє раціональному їх виконанню.

Як зазначає М. Зайцев, відсутність державної політики щодо забезпечення інформаційної безпеки та спеціального законодавства, яким передбачено напрямки її реалізації, зумовлює відсутність чіткої та узгодженої системи суб'єктів забезпечення інформаційної безпеки – органів, наділених відповідними завданнями і функціями та засобами для їх виконання, що має наслідком безконтрольний вплив на інформаційний простір держави та ставить під загрозу інформаційний суверенітет держави, заподіює шкоду всім суб'єктам інформаційних відносин, зокрема створює передумови для порушень прав людини та громадянина [4, с. 237].

У зв'язку з цим існує нагальна необхідність створення системи забезпечення інформаційної безпеки, при цьому, на думку вищеозначеного дослідника необхідно врахувати наступне: – по-перше, кількість елементів системи забезпечення інформаційної безпеки не повинна бути надмірною, оскільки їх збільшення буде призводити до ускладнення функціонування і, як наслідок, зменшення її ефективності; – по-друге, повинен існувати єдиний суб'єкт управління забезпеченням інформаційної безпеки, наділений владними повноваженнями у відношенні інших елементів забезпечення інформаційної безпеки та запроваджені ефективні механізми їх взаємодії; – по-третє, повноваження та функції суб'єктів забезпечення інформаційної безпеки повинні бути чітко розмежованими, не допускати дублювань з метою уникнення конкуренції в діяльності цих суб'єктів та, одночасно, охоплювати всі сфери та аспекти забезпечення інформаційної безпеки, що дозволить досягти прийнятної ефективності функціонування системи; – по-четверте, до складу системи забезпечення інформаційної безпеки повинні входити не тільки органи публічної влади, а й інституції громадянського суспільства, що дозволить однаково ефективно захищати в інформаційних відносинах інтереси не тільки держави, а й суспільства та громадян.

Низка пріоритетів розвитку національної інформаційної політики й інформаційної безпеки була сформульована у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» та у «Доктрині інформаційної безпеки України» від 8 липня 2009 р. Зокрема, у першому з вищеозначених законів, зазначається, що за умов швидкого розвитку глобального інформаційного суспільства, широкого використання ІКТ у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки. Інформаційна безпека − це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Вирішення проблеми інформаційної безпеки має здійснюватися за такими шляхами: створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань; вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація [5].

В свою чергу, більш детально напрямки інформаційної політики нашої держави та заходи щодо забезпечення інформаційної безпеки розкриті й конкретизовані у «Доктрині інформаційної безпеки України» від 8 липня 2009 р. Згідно цьому документу напрямки діяльності всіх суб'єктів інформаційної безпеки та інформаційної політики держави повинні бути такими: інформаційно-психологічний: забезпечення конституційних прав і свобод людини і громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей; технологічного розвитку: розбудова та інноваційне оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, обробки та поширення інформації; захисту інформації: забезпечення конфіденційності,

цілісності та доступності інформації, в тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак [6].

У вищеозначеній доктрині підкреслюється, що держава з метою забезпечення інформаційної безпеки України має вживати таких заходів: 1) у зовнішньополітичній сфері: вдосконалення інформаційного супроводу державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном; організаційно-технічне, інформаційне та ресурсне сприяння держави вітчизняним засобам масової інформації, що формують у світовому інформаційному просторі позитивний імідж України; посилення інформаційно-просвітницької діяльності серед населення щодо забезпечення національної безпеки України в разі повноправного її партнерства з державами − членами ЄС та НАТО; інтеграція в міжнародні інформаційно-телекомунікаційні системи та організації на засадах рівноправності, економічної доцільності та збереження інформаційного суверенітету; гарантування своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та їх нейтралізації; 2) у сфері державної безпеки: залучення засобів масової інформації до забезпечення неухильного додержання конституційних прав і свобод людини і громадянина, захисту конституційного устрою, вдосконалення системи політичної влади з метою зміцнення демократії, духовних та моральних засад суспільства; підвищення ефективності функціонування органів державної влади; підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; розвиток національної інформаційної інфраструктури на засадах стимулювання вітчизняних виробників і користувачів новітніми інформаційно-телекомунікаційними засобами і технологіями, комп'ютерними системами і мережами; 3) у воєнній сфері: проведення систематичного аналізу застосування засобів, форм та способів інформаційної боротьби у воєнній сфері, визначення напрямів забезпечення інформаційної безпеки держави; удосконалення законодавства з питань інформаційної безпеки, координації діяльності органів державної влади та органів військового управління під час вирішення завдань забезпечення інформаційної безпеки; удосконалення видів і засобів захисту інформації в інформаційно-телекомунікаційних мережах, що задіяні в управлінні військами і зброєю, від несанкціонованого доступу; удосконалення форм і способів протидії інформаційно-психологічним операціям, спрямованим на послаблення обороноздатності держави; підготовка спеціалістів з питань інформаційної безпеки у воєнній сфері; 4) у внутрішньополітичній сфері: створення дієвої та прозорої системи громадського контролю за діяльністю органів державної влади і органів місцевого самоврядування, громадсько-політичних структур, зокрема через створення системи Суспільного телебачення і радіомовлення України; поліпшення взаємодії органів державної влади з громадськими організаціями у сфері боротьби з проявами обмеження конституційних прав і свобод людини і громадянина та маніпулювання масовою свідомістю; 5) в економічній сфері: підтримка вітчизняних виробників високотехнологічної продукції, насамперед комп'ютерно-телекомунікаційних засобів і технологій; формування вітчизняної індустрії інформаційних послуг, підвищення ефективності використання державних, корпоративних і приватних інформаційних ресурсів; гармонізація законодавства України з питань інформаційної безпеки в економічній сфері з міжнародними нормами і стандартами; розроблення та вдосконалення методів і засобів захисту інформації; забезпечення сталого розвитку національного медіа-ринку під час впровадження в Україні цифрового телерадіомовлення; посилення державного контролю за додержанням вимог інформаційної безпеки в системах збирання, обробки, зберігання і передачі статистичної, фінансової, біржової, податкової та митної інформації; комплексна інформатизація процесів формування, розподілення і контролю за використанням бюджетних коштів; удосконалення системи статистичної звітності з метою підвищення оперативності, достовірності і релевантності звітної інформації; 6) у соціальній та гуманітарній сферах: формування та реалізація державної політики національного духовного та культурного відродження, яка відповідає інтересам Українського народу і визначає чіткі критерії і пріоритети формування інформаційної політики в соціальній сфері; запобігання монополізації національного інформаційного простору; вдосконалення законодавчого регулювання діяльності засобів масової інформації, зокрема, з метою підтримки діяльності, спрямованої на формування оптимістичної морально-психологічної атмосфери в суспільстві, популяризації національних культурних цінностей, сприяння соціальній стабільності і злагоді; державна підтримка вітчизняного виробника інформаційної продукції; у науково-технологічній сфері: забезпечення технологічної конкурентоспроможності України у сфері інформатизації та зв'язку; розвиток міжнародного науково-технічного співробітництва в сфері забезпечення захисту інформації у міжнародних телекомунікаційних системах;

удосконалення системи охорони та захисту права інтелектуальної власності; науково-технологічний супровід формування і розвитку в Україні інформаційного суспільства з урахуванням вимог забезпечення інформаційної безпеки України; розширення можливостей доступу громадян до світового інформаційного простору, зокрема до наукової та науковотехнічної інформації; 8) в екологічній сфері: проведення комплексного аналізу екологічного стану територій та їх виробничого потенціалу з метою вироблення інформаційної політики щодо впровадження концепції сталого розвитку; застосування сучасних аерокосмічних, комп'ютерно-телекомунікаційних та геоінформаційних засобів і технологій для комплексного моніторингу, профілактики і своєчасного реагування на надзвичайні ситуації; створення бази даних екологічно безпечних технологій і продукції, їх розробників, виробників і постачальників, результатів маркетингових досліджень екологічного ринку; підвищення рівня інформатизації галузі страхування для акумулювання коштів на відшкодування збитків від надзвичайних ситуацій, а також на довгострокове інвестування заходів із мінімізації ризиків життєдіяльності й господарювання [7].

Підсумки. Таким чином, ефективна інформаційна політика державних структур національної безпеки є запорукою захисту національного інформаційного простору і національних інтересів будь-якої країни. Перспективним напрямом подальших наукових розвідок є аналіз інтерактивної комунікації суб'єктів політичного процесу та її вплив на формування інформаційної політики.

Бібліографічний список:

1. Радковець Ю. Погляди на створення системи інформаційної безпеки України та її Збройних Сил. *Наука і оборона.* 2014. № 1. С. 38–42.

2. Закон України «Про основи національної безпеки». *ВВР України.* 2003. № 39. Ст. 351.

3. Інтерв'ю керівника Міністерства інформації Ю. Стеця від 3.12.2014 телеканалу Еспресо tv «У новостворюваному Міністерстві інформації України буде створено кілька департаментів, які займуться розробкою концепції інформаційної політики країни». URL: http://espreso.tv/news/2014/12/03/stec_rozpoviv__chym_bude_zaymatysya_ministerstvo_ informaciyi.

4. Зайцев М. Суб'єкти забезпечення інформаційної безпеки України. *Форум права.* 2013. № 3. С. 231–238.

5. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007– 2015 роки». *ВВР України.* 2007. № 12. Ст. 102.

6. Доктрина інформаційної безпеки України від 8 липня 2009 р. URL: http://zakon4.rada.gov.ua/laws/show/514/2009.

7. Доктрина інформаційної безпеки України від 8 липня 2009 р. URL: http://zakon4.rada.gov.ua/laws/show/514/2009.

References:

1. Radkovets Yu. Pohliady na stvorennia systemy informatsiinoi bezpeky Ukrainy ta yii Zbroinykh Syl. Nauka i oborona. 2014. № 1. S. 38–42.

2. Zakon Ukrainy «Pro osnovy natsionalnoi bezpeky». VVR Ukrainy. 2003. № 39. St. 351.

3. Interviu kerivnyka Ministerstva informatsii Yu. Stetsia vid 3.12.2014 telekanalu Espreso tv «U novostvorenomu Ministerstvi informatsii Ukrainy bude stvoreno kilka departamentiv, yaki zaimutsia rozrobkoiu kontseptsii informatsiinoi polityky krainy». URL: http://espreso.tv/news/2014/12/03/stec_rozpoviv__chym_bude_zaymatysya_ministerstvo_ informaciyi.

4. Zaitsev M. Subiekty zabezpechennia informatsiinoi bezpeky Ukrainy. Forum prava. 2013. № 3. S. 231–238.

5. Zakon Ukrainy «Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007– 2015 roky». VVR Ukrainy. 2007. № 12. St. 102.

6. Doktryna informatsiinoi bezpeky Ukrainy vid 8 lypnia 2009 r. URL: http://zakon4.rada.gov.ua/laws/show/514/2009.

7. Doktryna informatsiinoi bezpeky Ukrainy vid 8 lypnia 2009 r. URL: http://zakon4.rada.gov.ua/laws/show/514/2009.

Zaharenko K. V. Problems of formation of an effective public information policy

The activities of all involved in the field of information security of state structures should be well coordinated within the framework of common programs and plans, as well as certain functions.
The functioning of all state structures involved in the sphere of information security is analysed and it is indicated that their activities should be clearly coordinated within the framework of general programs and plans, as well as certain functions. Attention is paid to the fact that the modern information policy of Ukraine is characterized by inconsistency, lack of coordination in the activities of various authorities, lack of transparency in the adoption and implementation of political decisions. It is proposed for the effective implementation of programs in the field of information security, the state should provide the necessary

material resources, train specialists, develop the regulatory framework. Considering this, the Ukrainian legislation defines state structures that are subjects of national security. The priority directions of development of national information policy and information security of our state are formulated in the national doctrine of information security of Ukraine and enshrined in various laws.

For effective implementation of information security programs, the state should provide the necessary material resources to train professionals to develop a legislative framework. Taking this into account in the Ukrainian legislation specifies the governmental structures that are subject to national security. Priority directions of development of the national information policy and information security in our country formulated a national information security doctrine of Ukraine and enshrined in various laws. But the legislation on important issues of information security is still haphazard, and functions to ensure the information security policy and state dissipated among various entities is not conducive to their sustainable implementation. Thus, the functions and powers of government agencies to implement the information security should be provided with sufficient clarity and certainty.

Key words: *people, politics, information, culture, public policy, government institutions, legal framework, information security.*