ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 351.778.532:347

DOI <https://doi.org/10.32840/1813-3401-2019-4-42>

І. М. Базарко

кандидат наук з державного управління,
старший викладач кафедри публічного управління та адміністрування
Львівського національного університету ветеринарної медицини та
біотехнологій імені С. З. Гжицького

ДЕРЖАВНА ПОЛІТИКА ФОРМУВАННЯ СУЧАСНИХ ПІДХОДІВ З ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

У статті проаналізовано еволюцію державної політики національної безпеки із виконання пріоритетних завдань суспільного розвитку в Україні. Проблема захисту від інформації істотно складніша за проблему захисту інформації через те, що інформаційні загрози надзвичайно різноманітні, а їх вплив далеко не завжди є очевидним. Критерієм забезпечення інформаційної безпеки є наявність стану захищеності життєво важливих інтересів, які встановлюється за сукупністю ознак захищеності. Акцент на захист інформації під час використання інформаційних і комунікаційних технологій, що зберігся за інерцією з часів, коли власником інформації була тільки держава і вона ж вирішувала всі питання, пов'язані із захистом інформації, а чільним був аспект конфіденційності, що на цей час став архаїчним.

Досліджено особливості державного управління у сфері соціально-економічного розвитку щодо інформаційної безпеки в Україні на сучасному етапі. Щодо багатьох основоположних понять інформаційної безпеки, що стосуються її правового, організаційного та технічного забезпечення, триває наукова дискусія, невирішеними залишаються окремі проблеми стандартизації в області інформаційної безпеки. Рішенням специфічних завдань захисту інформації в сучасному кіберпросторі повинні займатися відповідні фахівці, які проектуєть, створюють і експлуатують комплексні системи захисту інформації від зовнішнього втручання.

Обґрунтовано запровадження комплексного підходу щодо правового регулювання обороноздатності держави в контексті національної безпеки. В переліку завдань, що вирішуються державою в сфері забезпечення інформаційної безпеки, є інтенсивний розвиток правового регулювання відносин у сфері протидії загрозам, закріплюються пріоритетні інтереси в інформаційній сфері, чому сприяє прийняття значної кількості законодавчих актів. Ці обставини зумовлюють обов'язковість вивчення основ правового забезпечення інформаційної безпеки, змістовним наповненням якого має стати уявлення про правове регулювання відносин в інформаційній сфері.

З'ясовано вплив процесів інформаційно-гібридного характеру на трансформацію державної політики в оборонній галузі України. З урахуванням темпів і масштабів впровадження комп'ютерів, всіляких гаджетів і телекомунікацій такі небезпеки різко зростають. Проблема

захисту від інформації є істотно складнішою за проблему захисту інформації через те, що інформаційні загрози надзвичайно різноманітні, а їх вплив далеко не завжди є очевидним. Критерієм забезпечення інформаційної безпеки є наявність стану захищеності життєво важливих інтересів, які встановлюється за сукупністю ознак захищеності.

Ключові слова: інформаційна безпека, органи державної влади, соціально-економічний розвиток, державна політика, обороноздатність України, національна безпека, сучасний етап, підвищення ефективності.

Постановка проблеми. Сучасні підходи до проблеми забезпечення інформаційної безпеки стали еволюційним розвитком вирішення завдань захисту інформації, які вирішувалися протягом багатовікової історії розвитку людської цивілізації різними методами і засобами. Забезпечення інформаційної безпеки в сучасних умовах повинно мати комплексний характер, як за цілями, так і за способами використання засобів [13]. Важливість інформаційної безпеки зумовлена високими темпами інформатизації усього суспільства, складними і неоднозначними процесами глобалізації щодо розвитку і впровадження сучасних інформаційних та комунікаційних технологій.

Розвиток інформаційних і комунікаційних технологій породжує все нові загрози, підходи до захисту від яких, як і раніше, мають здебільшого емпіричний характер. Підготовка кадрів у сфері інформаційної безпеки має суттєві особливості, оскільки виступає не тільки як реакція на попит ринку щодо таких фахівців, а й як важливий складник комплексу заходів держави щодо протидії загрозам в інформаційній сфері [1]. Основоположним у системі підготовки фахівців, чия професійна діяльність безпосередньо пов'язана із забезпеченням інформаційної безпеки і захисту інформації, є наявність державних стандартів і розроблених на їх базі основних програм у сфері інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Загальні підходи до аналізу інформаційної безпеки тісно корелюють із загальною теорією безпеки, основами безпечної життєдіяльності, а питання інформаційної безпеки ще не знайшли цілісного вираження в сучасній науці [11]. Дослідження у сфері інформаційної безпеки донедавна проводилися лише в закритих і військових вузах, а інформація про досягнення розвитку цієї наукової галузі не мала широкого поширення. Мета функціонування системи інформаційної безпеки зводиться до створення умов життєдіяльності об'єктів, що мають сферу життєво важливих інтересів.

Органами державної влади на законодавчому рівні основним способом забезпечення

інформаційної безпеки визначено захист життєво важливих інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз [6]. Незважаючи на широке вживання цього поняття, його сутність у науковому контексті глибоко не досліджена, а сутність і сфера застосування у нормативній, довідковій та науковій літературі однозначно поки що не визначена. Проблеми забезпечення інформаційної безпеки повинні вирішуватися в тісному взаємозв'язку з розробкою правового забезпечення процесів інформатизації, яке в ідеалі повинно мати прогностичний характер [3].

Мета дослідження – обґрунтування актуальності удосконалення та підвищення ефективності державної політики з інформаційної безпеки в контексті обороноздатності України на сучасному етапі.

Для цього слід вирішити такі завдання:

1. Проаналізувати еволюцію державної політики національної безпеки із виконання пріоритетних завдань суспільного розвитку в Україні.
2. Дослідити особливості державного управління у сфері соціального розвитку щодо інформаційної безпеки в Україні на сучасному етапі.
3. Обґрунтувати запровадження комплексного підходу щодо розвитку обороноздатності держави в контексті національної безпеки.
4. З'ясувати вплив процесів інформаційно-гібридного характеру на трансформацію державної політики в оборонній галузі України.

Виклад основного матеріалу. Актуальність інформаційної безпеки полягає в тому, що інформація здатна чинити такий вплив на людей і технічні комплекси, результати якого можуть мати негативний характер. Інформаційний вплив на людину, нав'язування шкідливої за своїми наслідками інформації, формування негативних звичок і смаків може викликати погіршення психічного стану, негативну поведінку [9]. З урахуванням темпів і масштабів впровадження комп'ютерів, всіляких гаджетів і телекомунікацій такі небезпеки різко зростають. Проблема захисту від інформації є істотно складнішою за проблему захисту інформації через те, що інформаційні загрози надзвичайно

різноманітні, а їх вплив далеко не завжди є очевидним.

Критерієм забезпечення інформаційної безпеки є наявність стану захищеності життєво важливих інтересів, які встановлюються за сукупністю ознак захищеності. Одночасно громадяни, громадські організації, держави виступають як суб'єкти правовідносин, що своїми діями здатні реалізувати належні їм права і обов'язки, і здатні відповідати за вчинені правопорушення, у тому числі у сфері інформаційної безпеки [5]. Як об'єкти інформаційної безпеки розглядаються окремі особистості, а також соціальні групи, спільності людей або ж інші громадські організації, що мають сферу життєво важливих інтересів.

До життєво важливих об'єктів громадянського суспільства належать громадські організації, матеріальні і духовні цінності, за допомогою яких забезпечується захист прав і свобод громадян. Життєво важливими об'єктами держави є її населення, територія та економіка, за допомогою яких забезпечується реалізація життєво важливих інтересів країни як суб'єкта міжнародного права [7]. Загрози об'єктів інформаційної безпеки виходять від внутрішніх і зовнішніх джерел небезпеки і являють собою сукупність негативних чинників, здатних під час впливу на життєво важливий об'єкт привести до подій і умов, за настання яких такий вплив реалізується.

Для забезпечення належного рівня інформаційної безпеки у всіх сферах життєдіяльності необхідна безпосередня і активна участь всіх учасників інформаційних процесів. Тому ефективне рішення проблеми інформаційної безпеки на всіх рівнях вимагає високоорганізованого кадрового забезпечення, тобто створення системи підготовки на регулярній основі фахівців різних спеціальностей, що володіють відповідним обсягом і рівнем знань і навичок забезпечення інформаційної безпеки [12]. Зміст проблем інформаційної безпеки повинен формуватися в суворій відповідності із сутністю проблем інформатизації, а концептуальні підходи до їх вирішення повинні бути взаємопов'язаними з концепціями інформатизації.

Забезпечення інформаційної безпеки держави, фірми, установи, групи суб'єктів, об'єднаних якимись відносинами, починається з формулювання завдання, визначення значущих інформаційних потоків, очікуваних взаємодій стосовно об'єкту середовища, аналізу загроз

і побудови системи захисту. Особливо слід відзначити незадовільну забезпеченість фахівцями структур державного управління, сфери економіки і фінансово-кредитних відносин. Повноцінно сформулювати завдання забезпечення інформаційної безпеки можуть тільки особи, які безпосередньо визначають стратегічні цілі, що захищаються, власники і топ-менеджери системи інформаційних потоків.

Крім вивчення проблематики інформаційної безпеки і захисту інформації, знання в цій галузі розвиваються і систематизуються. Для найширшої категорії фахівців, які є кінцевими користувачами сучасних інформаційних і комунікаційних технологій, весь спектр питань з інформаційної безпеки на цей час сконцентрований на інформаційних технологіях [10]. За багатьма основоположними поняттями інформаційної безпеки, що стосуються її правового, організаційного та технічного забезпечення, триває наукова дискусія, невирішеними залишаються окремі проблеми стандартизації в області інформаційної безпеки.

Акцент на захист інформації під час використання інформаційних і комунікаційних технологій, що зберігся за інерцією з часів, коли власником інформації була тільки держава і вона ж вирішувала всі питання, пов'язані із захистом інформації, а чільним був аспект конфіденційності, який на цей час став архаїчним [2]. Рішенням специфічних завдань захисту інформації в сучасному кіберпросторі повинні займатися відповідні фахівці, які проектують, створюють і експлуатують комплексні системи захисту інформації. Основним завданням реалізації аспектів інформаційної безпеки в багаторівневій системі інформаційної підготовки є підготовка з питань забезпечення інформаційної безпеки під час використання комп'ютерних засобів і інформаційних технологій.

Для звичайного користувача інформаційних і комунікаційних технологій рівень знань, умінь і навичок щодо застосування інформаційних і комунікаційних технологій повинен розглядатися в багаторівневому контексті. Для вирішення зазначених протиріч, формування професіоналізму, високої інформаційної культури, розвитку інформаційної підготовки в умовах широкомасштабного впровадження інформаційних і комунікаційних технологій, з урахуванням їх зростаючої різноманітності і ускладнення, підвищення рівня компетентності в області інформаційної безпеки і захисту

інформації є необхідною сучасною науковою основою [8].

Рівень інформаційної культури характеризує ефективність використання інформаційних ресурсів, адаптивність в інформаційному просторі, сформованому з використанням сучасних інформаційних і комунікаційних технологій за обов'язкового забезпечення вимог інформаційної безпеки. Інформаційна культура може бути уособлена як відносно цілісна підсистема загальної і професійної культури людини, що є результатом поетапного освоєння інформаційних і комунікаційних технологій, що у процесі інформаційної підготовки складається з декількох взаємопов'язаних структурних компонентів.

Практична частина інформаційної підготовки повинна бути спрямована на формування міцних навичок забезпечення інформаційної безпеки під час використання в комп'ютерних системах і мережах можливостей загального і спеціального програмного забезпечення, загальнонавчаних засобів захисту інформації [4]. В переліку завдань, що вирішуються державою в сфері забезпечення інформаційної безпеки, є інтенсивний розвиток правового регулювання відносин у сфері протидії загрозам, закріплюються пріоритетні інтереси в інформаційній сфері, чому сприяє прийняття значної кількості законодавчих актів. Ці обставини зумовлюють обов'язковість вивчення основ правового забезпечення інформаційної безпеки, змістовним наповненням якого має стати уявлення про правове регулювання відносин в інформаційній сфері.

Висновки. Концепція інформаційної безпеки повинна ґрунтуватися на розумінні призначення, ролі та цілей цих знань, трактуванні способів їх відображення в якості обов'язкового складника інформаційної підготовки, і представляти собою систему поглядів на основні завдання, принципи формування і напрями розвитку методичної системи навчання інформаційної безпеки. Для виявлення структури системи, типізації зв'язків, аналізу і визначення компонентів, оптимізації інформаційного середовища найбільш продуктивним є системний підхід.

Поряд з традиційно розглянутими аспектами інформаційної безпеки і захисту інформації, в ній повинні знайти відображення методологічні, правові, організаційно-управлінські аспекти інформаційної безпеки. В контексті інформаційної безпеки повинні бути розглянуті проблеми комп'ютерної етики, що виникають

у зв'язку з відсутністю ясності в питаннях про те, якими мають бути етичні обмеження під час застосування комп'ютерних технологій. Одним з основних результатів дослідження інформаційної безпеки повинно бути усвідомлення того, що безпека інформаційних систем є результатом діалектичної взаємодії деструктивних факторів та механізмів комплексної системи захисту інформації, що забезпечує їх запобігання, блокування, усунення, мінімізацію ризиків.

Список використаної літератури:

1. Акімова Л.М. Теоретичні основи державного управління розвитком національної безпеки. *Державне управління: удосконалення та розвиток: електрон. наук. фах. вид.* 2015. № 5. URL: <http://www.dy.nayka.com.ua/?op=1&z=1210> (дата звернення 09.12.2019).
2. Державний сектор і функції держави у період кризи / О.Й. Пасхавер, Л.Т. Верховодова, О.М. Кошик та ін. Київ : СПД Моляр С.В. 2009. 130 с.
3. Концептуальні засади розвитку системи забезпечення національної безпеки України: аналіт. доп. / О.О. Резнікова, В.Ю. Цюкало, В.О. Паливода та ін. Київ : НІСД. 2015. 58 с.
4. Костюк І. Державне управління в Україні в період реалізації адміністративної реформи: основні поняття та категорії. *Державне управління та місцеве самоврядування*. 2013. URL: http://nbuv.gov.ua/j-pdf/dums_2013_1_9.pdf.
5. Кунц Г. Управление: системный и ситуационный анализ управленческих функций / пер. с англ. в 2 т. / Общ. ред. акад. Д.М. Гвишиани. Москва: Прогресс, 2017, Т.1. 497с.
6. Лекарь С.І. Поняття та зміст економічної безпеки. *Форум права*. 2012. № 2. С. 49–51.
7. Малишко В.М. Актуальні проблеми економічної безпеки в системі національної безпеки України. *Юридичний вісник. Повітряне і космічне право*. 2015. № 4. С. 29–37.
8. Методичні рекомендації щодо розрахунку рівня економічної безпеки України, затверджені Наказом Міністерства економічного розвитку і торгівлі від 29.10.2013 р. № 1277. URL: <http://www.me.gov.ua> (дата звернення 18.11.2019).
9. Парубчак І.О. Теоретико-методологічні підходи до формування державної антикорупційної політики в контексті національної безпеки України. *Теорія та практика державного управління та місцевого самоврядування: електр. наук. фах. вид. Херсонського національного технічного університету*. 2017. № 2. URL: http://el-zbirn-du.at.ua/2017_2/34.pdf. URL: (дата звернення 13.10.2019).
10. Резнікова О.О., Цюкало В.Ю., Паливода В.О., Дрьомов С.В., Сьомін С.В. Концептуальні

- засади розвитку системи забезпечення національної безпеки України: Аналіт. доп. Київ : НІСД, 2015. 58 с.
11. Скорук О.В. Економічна безпека держави: сутність, складові елементи та проблеми забезпечення. Науковий вісник Ужгородського національного університету: Сер.: Міжнародні економічні відносини та світове господарство. Ужгород: Видавничий дім «Гельветика», 2016. Вип. 6. Ч. 3. С. 34–40.
 12. Стеценко С.П. Економічна безпека: сутність і структура. Інвестиції: практика та досвід. 2013. № 24. С. 113–117.
 13. Шайдоров О.І. Економічна безпека в системі національної безпеки. Університетські наукові записки. 2011. С. 395–400.

Bazarko I. M. State policy of formation of modern approaches for increasing the efficiency of information security in the context of Ukraine's national defense capability

The article analyzes the evolution of national security policy to fulfill the priorities of social development in Ukraine. The problem of information security is more complicated than the problem of information security because information threats are extremely diverse and their impact is not always obvious. The criterion for ensuring information security is the existence of a state of security of vital interests, which is established by a set of security features. The emphasis on information security in the use of information and communication technologies, preserved inertia from a time when the owner of the information was only the state, and it also resolved all issues related to the protection of information, and a prominent aspect of privacy, is now archaic.

The peculiarities of public administration in the field of social and economic development regarding information security in Ukraine at the present stage are investigated. In many fundamental concepts of information security, concerning its legal, organizational and technical support, scientific debate continues, and some problems of standardization in the field of information security remain unresolved. Specific information security challenges in today's cyberspace should be handled by appropriate professionals who design, create and operate integrated systems for protecting information from external interference.

The introduction of a comprehensive approach to the legal regulation of the state's defense capability in the context of national security is substantiated. The list of tasks to be resolved by the state in the field of information security is the intensive development of legal regulation of relations in the field of counteraction to threats, the priority interests in the information sphere are fixed, which is facilitated by the adoption of a large number of legislative acts. These circumstances make it compulsory to study the basics of legal security of information security.

The influence of information-hybrid processes on the transformation of state policy in the defense sector of Ukraine is investigated. Given the pace and scale of computer deployment, all kinds of gadgets and telecommunications, these dangers are increasing dramatically. The problem of information security is more complicated than the problem of information security because information threats are extremely diverse and their impact is not always obvious. The criterion for ensuring information security is the existence of a state of security of vital interests, which is established by a set of security features.

Key words: information security, public authorities, socio-economic development, state policy, defense capability of Ukraine, national security, current stage, efficiency gains.