DOI 10.52363/2414-5866-2021-1-49
УДК 351:342.57

Малахов Р. В. *аспірант ННВЦ НУЦЗ України*
ORSID: 0000-0002-5237-6742

Malakhov Roman *graduate student of National University of Civil Defence of Ukraine*

СТАНОВЛЕННЯ МЕХАНІЗМІВ ЗАПОБІГАННЯ МЕДІАЗАГРОЗАМ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

FORMATION OF MEDIA THREATS MECHANISMS PREVENTION IN THE NATIONAL SECURITY SYSTEM

В статті проаналізовано становлення механізмів запобігання медіазагрозам в системі національної безпеки. Здійснено характеристику існуючих ризиків в системі національної інформаційної безпеки, їхній вплив на розвиток соціуму та інформаційного середовища , а також економіку держави.

Виявлено умови реалізації інформаційної безпеки, які носять амбівалентний характер. З одного боку, саме держава являється і залишатиметься основним суб'єктом забезпечення інформаційної безпеки усіх учасників інформаційних стосунків. З іншого боку, ефективне рішення проблем забезпечення інформаційної безпеки, . захисту усіх категорій суб'єктів, прямо або що побічно беруть участь в процесах інформаційної взаємодії, від нанесення їм будь-якого збитку (матеріального, морального і т. д.) в результаті випадкових або умисних дій на інформацію і систему її обробки і передачі, тісно пов'язано з дотриманням основних прав громадян і інших суб'єктів інформаційних стосунків в цій сфері.

У роботі здійснений теоретико-методологічний аналіз політичного аспекту інформаційної безпеки в умовах становлення глобального інформаційного суспільства. Виявлені соціально-політичні наслідки інформатизації українського суспільства в контексті забезпечення інформаційної безпеки як окремих громадян, так і держави в цілому.

Інформаційна сфера, будучи системотворним чинником життя сучасного суспільства, активно впливає на стан політичною економічною, оборонною і інших складових безпеки держав, що посилює все більшу значущість інформаційної безпеки в загальній системі національної безпеки.

Основним суб'єктом забезпечення інформаційної безпеки в сучасній Україні залишається держава.

Ключові слова: *інформаційне суспільство, національна безпека сучасної України, демократизація суспільства, державна політика, механізми запобігання медіазагрозам, ризики інформаційного середовища*.

The paper analyzes the formation of media threats mechanisms prevention in the national security system. The characterization of the existing risks in the national information security system, their impact on the development of society and the information environment, as well as the state's economy, was carried out.

The conditions for the information security implementation with ambivalent nature have been revealed. On the one hand, the state is and will remain the main subject of ensuring information security of all participants in information relations. On the other hand, an effective solution to the problems of ensuring information security, protecting all categories of subjects, directly or indirectly participating in the processes of information interaction, from causing them any damage (material, moral, etc.) as a result of accidental or intentional actions on information and the system of its processing and transmission, is closely related to the observance of the basic rights of citizens and other subjects of information relations in this area.

The paper provides a theoretical and methodological analysis of the political aspect of information security in the conditions of the formation of a global information society. The socio-political consequences of Ukrainian society informatization in the context of ensuring information security of both individual citizens and the state as a whole are revealed.

The information sphere, being a system-forming factor in the life of modern society, actively affects the state of political, economic, defense and other components of state security, which increases the increasing importance of information security in the general system of national security. The state remains the main subject of ensuring information security in modern Ukraine.

Keywords: *information society, national security of modern Ukraine, democratization of society, state policy, mechanisms for media threats preventing, the information environment risks.*

Постановка проблеми. Аналіз великого числа закордонних матеріалів, пов'язаних із забезпеченням національної безпеки, показує, що між вітчизняною і зарубіжною управлінською наукою, а також декларованими принципами і практикою є істотні відмінності. Основна відмінність полягає в тому, що в зарубіжних країнах національна безпека розглядається як переважно сфера оборони і державної безпеки. В Україні до недавнього часу домінував підхід до безпеки як до багатогранного явища, складовими частинами якого є

політична, військова, соціально-економічна, технологічна, культурна, інформаційна і інші види безпеки.

Розглядаючи інформаційне суспільство з точки зору соціальних технологій, є актуальним виявлення теоретичних і методологічних основ функціонування такого суспільства, його проблем і перспектив розвитку в плані формування і корекції наявних і потенційних закономірностей існування, зв'язаних саме з соціальними нормами і імперативами, тим самим підходячи до проблематики регулювання процесів формування інформаційної безпеки соціуму з соціально-управлінських позицій.

Аналіз останніх досліджень і публікацій Серед теоретичних джерел, в яких піднімалися проблеми державного регулювання інформаційного простору в системі національної безпеки в загальному плані, найбільшої увагу заслуговують роботи і дослідження [1, 2, 3, 4, 5,6, 7].

Мета і завдання дослідження Становлення механізмів запобігання медіазагрозам в системі національної безпеки.

Виклад основного матеріалу. Розвиток інформаційного суспільства на сучасному етапі ставить питання не лише про формати його функціонування, але і про механізми захисту, необхідні для успішної еволюції суспільства і збереження його внутрішніх і зовнішніх взаємозв'язків, що впливають на поступальність процесів розвитку. Термін «інформаційна безпека» має на увазі тлумачення як з точки зору захисту (пасивний елемент), так і формування безпеки (проактивна діяльність). Під цим терміном зазвичай розуміють обмеження на користування інформаційними потоками, створення і використання контрінформаційних технологій відносно інформаційних загроз на адресу суб'єкта, захист технічних носіїв і банків інформації, психофізичну інформаційну безпеку, нарешті, синтез усіх або ряду перерахованих дій [6].

Проблеми інформаційної безпеки тісно пов'язані з соціальною безпекою, вивчення інформаційної безпеки в соціологічному аспекті сприяє забезпеченню розвитку інформаційного соціуму. Інформаційна безпека стала однією із складових національної безпеки, її обговорення вийшло на міждержавний рівень.

Нарешті, соціологічний аналіз інформаційної безпеки значимий для організацій з точки зору запобігання можливого розкрадання або порушення їх власних інформаційних ресурсів, інсайдерських загроз і з точки зору інформаційних атак на імідж, репутацію, честь і гідність організації або її конкретних фігурантів.

Можна констатувати переважання технічних підходів в інформаційній безпеці і недооцінку соціологічного аналізу цієї проблематики. З цим пов'язана недостатня соціологічна опрацьованість питань інформаційної безпеки і її ролі в захисті інтересів соціуму в інформаційному середовищі. При

усій відмінності підходів дослідників і учених до поняття інформаційної безпеки, думається, варто відмітити, що це поняття вживається до різних об'єктів і процесів сучасного інформаційного суспільства, яким загрожують різні ризики, загрози і небезпеки інформаційно-комунікаційного характеру. І тут дуже чітко можна простежити аналогію з подібним соціологічним тлумаченням підходів до загального поняття безпеки. Так, різним природним і соціальним об'єктам і процесам загрожують як екологічні, техногенні, виробничі, так і антропогенно-соціальні небезпеки.

Інформаційна безпека є відносно новим елементом в системі національної безпеки. Поява цього елементу як поняття і явища цілком пов'язано з процесами створення глобального інформаційного простору і формуванням такого ж глобального інформаційного суспільства, що зумовлено якісним етапним переходом людської суспільно-економічної формації з суспільства індустріального в суспільство постіндустріальне, яке де-факто вже іменується інформаційним суспільством. Глобальне інформаційне суспільство припускає необхідність виникнення і функціонування національних інформаційних суспільств, якщо держави, що акумулюють в собі ті або інші соціуми, не вважають за краще залишитися на задвірках еволюції загальносвітового процесу, що безперервно відбувається [7].

Сьогоднішній день характеризується активним і безповоротним входженням в життєдіяльність особи, суспільства і держави інформаційно-комунікаційних технологій, новітніх інформаційних систем, що чинять в зростаючому ступені глибоку дію на усі сфери людських, громадських і державних інтересів. Що нещодавно висувалися як нові поняття «інформаційна революція», «інформаційне суспільство», «інформаційна безпека» сьогодні стали звичними і адаптованими до реалій сучасності не лише фахівців і учених, але і рядових споживачів інформації.

Під інформаційною безпекою нині розуміється стан належної захищеності особи, суспільства, держави від ризиків, загроз і небезпек, що мають інформаційну природу.

Слід врахувати, що якісна константа глобального інформаційного суспільства знаходиться в безперервному процесі вдосконалення. Диктат інформаційно-комунікаційних технологій все активніше впливає на соціальні процеси. Широке використання комп'ютерних і інформаційних систем і технологій - від рядового користувача з державних управлінських структур, включаючи і силові відомства, відкриває небачені раніше можливості не лише інформаційного обміну і пізнання дійсності, але і якісно нові можливості кримінального характеру (хакерство, зломи електронних і комп'ютерних систем з метою економічного і політичного шантажу, в цілях здійснення терористичної і екстремістської діяльності і так

далі).

На наш погляд, віддаючи належне техніко-технологічним аспектам інформаційної безпеки, все ж слід враховувати і соціальні аспекти інформаційної безпеки, тому що саме вони якраз і можуть успішно протистояти негативному, дестабілізуючому і деструктивному інформаційному вмісту, що закладається в інформаційно-комунікаційні технології з метою відповідної дії на особу, суспільство і інтереси держави[1].

Інформаційна безпека розглядається як стан захищеності інформаційного середовища соціуму, що забезпечує її формування, , використання і розвиток в інтересах особи, суспільства, держави. Отже, інтереси особи, суспільства і держави, повинні бути враховані в нинішній Стратегії національної безпеки України, як сукупне забезпечення конституційних прав і свобод, особистої безпеки, підвищення рівня життя, фізичний, духовний і інтелектуальний розвиток можуть і мають бути захищені і в цьому аспекті. Очевидно, що інтереси особи і суспільства ув'язуються з розвитком демократії і створенням правової держави, а також в досягненні і підтримці громадської згоди, нарешті, в духовному оновленні і розвитку України. Інтереси ж країни криються в непорушності конституційного ладу, суверенітету і територіальної цілісності України, в політичній, економічній і соціальній стабільності, у безумовному забезпеченні законності і підтримці правопорядку, в розвитку міжнародної співпраці. З цього виходить, що зміцнення інформаційної безпеки в системі національної безпеки України одне з найважливіших довгострокових завдань. Роль інформаційної безпеки і її місце в системі національної безпеки визначаються також тим, що державна інформаційна політика тісно взаємодіє з державною політикою забезпечення національної безпеки України через систему інформаційної безпеки, де остання виступає важливою сполучною ланкою усіх основних компонентів державної політики в єдине ціле.

Усе вищесказане, в цілому, і зумовлює місце інформаційної безпеки в системі національної безпеки держави.

Таким чином, якщо національна безпека як складне багатофункціональне явище, що являє собою систему взаємозв'язаних елементів, і ця система включає заявлену сукупність стратегічних і концептуальних принципів, установок і положень певних соціально-політичних інститутів і організацій відповідних засобів, методів і способів, що дозволяють превентивно або адекватно реагувати на ризики, загрози і небезпеки, то інформаційна безпека в межах своєї компетенції охоплює одну з пріоритетних сфер життєдіяльності людей - інформаційне середовище, яке являється на сьогодні одним з найважливіших елементів загальної системи національної безпеки, і покликана належним чином забезпечувати політичні, економічні, морально-духовні і інші соціальні права і інтереси, матеріальні і нематеріальні блага особи, суспільства

і держави [4].

Розвиток інформаційного суспільства, соціальне самопочуття його членів повинно спиратися на деякі загальновстановлені критерії і правила що визначають захист матеріальних і нематеріальних благ учасників такого суспільства. Ці критерії і правила в сукупності складають інформаційну безпеку. Нині багатьма дослідниками і фахівцями саме питання інформаційної безпеки висуваються на перший план як необхідний і безумовний чинник успішного формування і функціонування інформаційного суспільства. І не лише ними. Питання інформаційної безпеки вийшли і на державний рівень.

Під інформаційною безпекою сьогодні зазвичай розуміється захищеність інформації і підтримувальної її інфраструктури від будь-яких випадкових або обдуманих і зловмисних дій, результатом яких може стати нанесення збитку самій інформації, її власникам або підтримувальній інфраструктурі.

Завдання інформаційної безпеки, таким чином, зводяться до мінімізації збитку, прогнозування і запобігання таким діям.

Інформаційна безпека, крім того, є сукупністю найрізноманітніших стосунків, що містять в якості абсолютного безумовного елементу безпосередньо сам інформаційний компонент, представлений рядом термінів, використовуваних правовими нормами, зокрема, нормами цивільного права і кримінального права. Досить предметно інформаційну безпеку характеризують такі елементи складу злочину як предмет і діяння. Так, до предмета злочинів в інформаційній сфері відносяться (вказують на нього) такі терміни, як: «відомості», «дані», «таємниця», «документи», «матеріали» «технологія», «факти», «суть», «носій», «засоби зв'язку» і так далі. До протиправному діянню проти інформаційної безпеки можуть бути віднесені наступні терміни: як «розголошування», «поширення» «публікація», «оголошення», «рекламування», «демонстрація», «видання», «наклеп», «привласнення», «заклик», «фальсифікація» і так далі. З урахуванням викладеного, очевидно, що інформаційна безпека як об'єкт кримінально-правової охорони не лише існує в кримінальному праві, але і є поширеним об'єктом кримінально-правової охорони[2].

Слід зазначити, що поняття інформаційної безпеки визначення її формулювання тими або іншими авторами істотно різняться, але саме - в точності і інтерпретаціях самих формулювань сенс же залишається незмінним.

Розглядаючи інформаційну безпеку як стан захищеності інформаційного середовища, слід припустити наявність складових інформаційної безпеки : поняття інформаційної середовища дуже містке, і в ньому існують відособлені і інтегровані один у одного інформаційні простори. На сьогодні виробилася загальна характеристика інформаційної безпеки. У сучасному соціумі інформаційна сфера має дві складові: інформаційно-технічну

(штучно створений людиною світ техніки, технологій і т. п.) і інформаційно-психологічну (природний світ, включаючи індивіда). В цілому, інформаційну безпеку можна представити двома елементами: інформаційно-технічною і інформаційно-психологічною (психофізичною).

Інформаційно-технічна (ще її можна назвати технологічною) частина інформаційної безпеки забезпечує захист її технічних і технологічних аспектів. Під технічним захистом розуміється забезпечення захисту не криптографічними методами інформації, що містить відомості, та становлять державну таємницю, інформації з обмеженим доступом, запобігання її витоку по технічних каналах, несанкціонованого доступу до неї, спеціальних дій на інформацію і носії інформації в цілях її добування, знищення, спотворення і блокування доступу на території України [3].

Висновки. Таким чином, інформаційні технології є важливим чинником інформатизації політичних стосунків, політичного процесу. У політичному процесі інформаційні технології виступають як комплекс інформаційних середовищ, владних структур, політичних інститутів, громадян, що утворюють цілісну систему, пов'язану за допомогою інформаційних потоків із зовнішніми по відношенню до політики громадськими процесами.

В умовах інформатизації, продовженням розвитку загальної теорії демократії є поява концепції «електронної демократії». Проте, існуючий розрив між потенційними можливостями, витікаючими з цієї концепції, і практичною реалізацією її ідей, обумовлений неоднозначним розумінням її суті науковими колами, політичними елітами і громадянами; а також принципово різними интересами учасників політичного процесу відносно цілей її практичної реалізації.

Включення інтернету в процеси інформаційної взаємодії у сфері політики стало можливим завдяки усвідомленню політичними акторами потенційних можливостей мережі. Технологічні інновації якісно змінюють інформаційне середовище існування політики, сприяючи наданню їй властивостей віртуальності, інтерактивності, глобальності, зв'язаності, стійкості. Постійні технологічні зміни в інтернеті провокують появу нових політичних практик.

Список використаних джерел:

1. Бебик В.М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблік рилейшинз. Київ : МАУП, 2005. 440

2. Дрешпак В.М. Структура та функції комунікативної підсистеми державного управління. Аспекти публічного управління. 2013. № 1. С. 22–27.

3. Романенко Є. Комунікація як необхідна складова розвитку

сучасного суспільства. Демократичне врядування. 2012. Вип. 9. URL: http://www.lvivacademy. com/visnik9/fail/Romanenko.pdf.

4. Ситник С. Інституалізація публічної політики. Політологічний вісник : зб. наук. пр. 2011. Вип. 52. С. 210-218.

5. Трегуб К.С. Особливості функціонування мас-медіа у період трансформації сучасного українського суспільства: проблема соціальної відповідальності. Вісник Львівського університету. 2015. Вип. 9. С. 138–146. URL:http://nbuv.gov.ua/UJRN/Vlnu_sociology_2015_9_16.

6. Тогобицька В.Д. Основні ризики впливу цифровізації економіки на соціально-економічні системи. *Вісник Національного університету цивільного захисту України (Серія: Державне управління)*. 2018. Вип. 1 (8). С. 14–23.

7. Харченко Л. С. Інформаційна безпека України : глосарій / Л. С. Харченко, В. А. Ліпкан, О. В. Логінов ; за загальною редакцією доктора юридичних наук, професора Р. А. Калюжного. Київ : Текст, 2011. 180 с.

References:

1. Bebyk V.M. Informatsiino-komunikatsiinyi menedzhment u hlobalnomu suspilstvi: psykholohiia, tekhnolohii, tekhnika pablik ryleishynz. Kyiv : MAUP, 2005. 440

2. Dreshpak V.M. Struktura ta funktsii komunikatyvnoi pidsystemy derzhavnoho upravlinnia. Aspekty publichnoho upravlinnia. 2013. № 1. S. 22–27.

3. Romanenko Ye. Komunikatsiia yak neobkhidna skladova rozvytku suchasnoho suspilstva. Demokratychne vriaduvannia. 2012. Vyp. 9. URL: http://www.lvivacademy. com/visnik9/fail/Romanenko.pdf.

4. Sytnyk S. Instytualizatsiia publichnoi polityky. Politolohichnyi visnyk : zb. nauk. pr. 2011. Vyp. 52. S. 210-218.

5. Trehub K.S. Osoblyvosti funktsionuvannia mas-media u period transformatsii suchasnoho ukrainskoho suspilstva: problema sotsialnoi vidpovidalnosti. Visnyk Lvivskoho universytetu. 2015. Vyp. 9. S. 138–146. URL:http://nbuv.gov.ua/UJRN/Vlnu_sociology_2015_9_16.

6. Tohobytska V.D. Osnovni ryzyky vplyvu tsyfrovizatsii ekonomiky na sotsialno-ekonomichni systemy. Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy (Seriia: Derzhavne upravlinnia). 2018. Vyp. 1 (8). S. 14–23.

7. Kharchenko L. S. Informatsiina bezpeka Ukrainy : hlosarii / L. S. Kharchenko, V. A. Lipkan, O. V. Lohinov ; za zahalnoiu redaktsiieiu doktora yurydychnykh nauk, profesora R. A. Kaliuzhnoho. Kyiv : Tekst, 2011. 180 s.