DOI 10.52363/2414-5866-2021-2-51
УДК 351:342.57

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

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

РЕГІОНАЛЬНОЇ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЯК СКЛАДОВІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

REGIONAL INFORMATION SECURITY SYSTEM AS A COMPONENT OF NATIONAL SECURITY OF UKRAINE

Анотація. *В статті проаналізовано регіональну систему інформаційної безпеки, як складову національної безпеки України. Визначено, що будь яке інформаційне суспільство несе з собою не тільки нові рішення та можливості, а й нові загрози і ризики. Як і будь-яке інше, інформаційне суспільство недосконале, а інформаційно-комунікаційні технології – нейтральні. Наслідки їх застосування залежать від ціннісних настанов і державно-політичних рішень. Реалізація можливостей інформаційного суспільства – питання адекватної політики й своєчасних державно-управлінських рішень.*

Досліджено методологічні основи інформаційного забезпечення державної політики безпеки держави, класифіковано методи оцінювання, отримання, подачі інформації при здійсненні інформаційної безпеки, розкрито значення інформаційної безпеки в державно-управлінських відносинах у контексті процесів демократизації суспільства, охарактеризовано роль державно-управлінських інститутів як ключових суб'єктів реалізації інформаційної політики забезпечення національної безпеки сучасної України. В статті констатовано, що проблеми та питання, що стосуються інформаційного забезпечення безпеки держави (зокрема, щодо шляхів цього забезпечення), не є новими для дослідників – їх постійно порушують в усіх країнах світу науковці з різними науковими інтересами, які можуть торкатися цієї теми як прямо, так і опосередковано.

Ключові слова: *інформаційне суспільство, національна безпека сучасної України, демократизація суспільства, державна політика.*

Abstract. *The paper analyzes the regional information security system as a*

component of Ukraine's national security. It was determined that any information society brings with it not only new solutions and opportunities, but also new threats and risks. Like any other, the information society is imperfect, and information and communication technologies are neutral. The consequences of their application depend on value guidelines and state and political decisions. Realization of the information society possibilities is a matter of adequate policy and timely state-management decisions.

The methodological foundations of the information provision of the state security policy of the state were studied, the methods of evaluating, obtaining, submitting information in the implementation of information security were classified, the importance of information security in state-management relations in the context of the processes of democratization of society is revealed, the role of state-management institutes as key subjects of the implementation of the information policy of ensuring national security of modern Ukraine is characterized. The paper states that the problems and questions related to the information security of the state (in particular, the ways of this security) are not new for researchers - they are constantly raised in all countries of the world by scientists with various scientific interests who can touch this topic as directly , and indirectly.

Keywords: *information society, national security of modern Ukraine, democratization of society, state policy.*

Постановка проблеми. Найважливішою підсистемою регіональної системи інформаційної безпеки є її підсистема управління. По суті, вона є ядром цієї системи й об’єднує об’єктні (цільові) та функціональні підсистеми в єдине ціле. Тому інтегральну характеристику підсистеми управління відображають показники ефективності розглядуваної системи в цілому. У зв’язку з тим, що головною метою системи забезпечення інформаційної безпеки є захист об’єктів, інтегральним показником системи управління цією безпекою може служити ступінь її впливу на ефективність захисту об’єктів або на частку (кількість) об’єктів, на яких виконуються встановлені вимоги до забезпечення такої безпеки.

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].

Мета і завдання дослідження: проаналізувати регіональної системи інформаційної безпеки, як складові національної безпеки України.

Виклад основого матеріалу. Зауважимо, що через складність регіональних систем інформаційної безпеки опосередкований вплив підсистеми

управління нею на процеси її забезпечення на конкретному об’єкті захисту є проблематичним, відповідно, оцінити цей показник неможливо [4]. Тому пропонується використовувати окремі показники, що характеризують ступінь виконання окремих функцій підсистемою управління, без яких управління не є можливим.

До зазначених функцій належать такі:

1) створення організаційної структури органів управління регіональними системами інформаційної безпеки;

2) розроблення раціональних норм і правил, що регламентують відносини між елементами такої регіональної системи;

3) інформаційне забезпечення діяльності органів таких систем необхідними нормативними, методичними тощо документами з питань забезпечення цієї безпеки;

4) інформаційне забезпечення органів управління цими системами, потрібне для ухвалення своєчасних адекватних рішень, серед іншого за результатами моніторингу стану розглядуваних регіональних систем і контролю виконання чинних норм і правил;

5) планування розвитку регіональних систем інформаційної безпеки, відштовхуючись від їх поточного стану, реалізація планів їх розвитку;

6) безпосереднє управління процесами забезпечення такої безпеки на конкретних об’єктах [3].

Підкреслимо, що організаційна структура підсистеми управління регіональної системи інформаційної безпеки охоплює органи управління всією системою й органи управління в об’єктних і функціональних підсистемах. Оскільки вимоги до їх складу задані в чинних законодавчих та організаційно-розпорядчих документах, то як показник оцінювання стану організаційної структури пропонується використовувати повноту формування цієї структури.

Результатом виконання другої функції є система документів у сфері забезпечення інформаційної безпеки, які встановлюють норми і правила регламентації відносин у цій галузі. Оцінювання стану розвитку системи документів пропонується здійснювати на двох рівнях.

Зокрема, на нижньому рівні необхідно оцінити, наскільки повно виконання функцій різних органів регіональної системи інформаційної безпеки в типових ситуаціях захисту інформації регламентовано правовими, організаційними і технічними нормами і правилами, а також забезпечено необхідною інформацією. Показники повноти регламентації і забезпечення функцій, що виконуються органами таких систем (із диференціацією за видами органів і їх функціями) використовуються для виявлення недоліків у чинних

документах, визначення необхідності їх доопрацювання або розроблення нових документів [1].

Для розрахунку цих показників необхідно попередньо згенерувати повну не надмірну безліч відносин у сфері інформаційної безпеки, для яких потрібні регламентація й інформаційного забезпечення.

На верхньому рівні як показник оцінювання стану системи документів пропонується використовувати повноту розроблення документів щодо необхідного складу (з диференціацією за видами документів). Такий показник потрібен для обґрунтування програм розроблення системи документів у розглядуваній сфері.

Іншою значущою функцією підсистеми управління регіональною системою інформаційної безпеки є організація інформаційного забезпечення діяльності органів системи забезпечення цієї безпеки, включно з доведенням до відома всіх органів необхідних документів у відповідній сфері, а також збирання інформації про стан підсистем її забезпечення та процесів, що в них відбуваються.

Також стан інформаційного забезпечення діяльності органів регіональної системи інформаційної безпеки можна оцінювати за допомогою такого показника, як повнота забезпечення цих органів необхідними для їх діяльності документами.

Водночас про цей стан багато що говорить оцінювання повноти і своєчасності надання інформації про стан об’єктних і функціональних підсистем розглядуваних регіональних систем.

Важлива для управління регіональною системою інформаційної безпеки функція контролю виконання чинних у цій системі норм і правил (вимог) реалізується відповідною функціональною підсистемою. При цьому стан підсистеми контролю характеризується часткою проконтрольованих об’єктів від загальної кількості об’єктів, які слід проконтролювати за певний період часу (повнотою виконання необхідних завдань контролю об’єктів). Необхідна кількість контрольованих об’єктів за заданий період часу, наприклад протягом місяця, визначається з урахуванням прогнозованої динаміки виникнення передумов до порушення після чергового акту контролю і необхідності своєчасного припинення цих порушень.

У цілому ступінь виконання функції управління розвитком регіональної системи інформаційної безпеки доцільно оцінювати за двома показниками:

1) за наявністю в органах управління системою забезпечення інформаційної безпеки обґрунтованих цілей завдань і необхідних результатів розвитку системи, а також програм і планів їх досягнення на короткострокову і довгострокову перспективи;

2) за повнотою реалізації цих програм і планів [1, с.78].

Указані вище показники оцінювання стану систем забезпечення інформаційної безпеки потрібні для об'єктивної характеристики процесів, що в них відбуваються, а також для виявлення наявних або можливих проблем і суперечностей. Їх виявлення може ґрунтуватися на порівнянні показників оцінювання стану розглядуваних систем з деякими еталонними значеннями (критеріями), характерними для різних якісно заданих градацій інтегральних оцінок стану системи.

Під критеріями оцінювання стану регіональної системи інформаційної безпеки розуміються порогові значення сукупності показників оцінювання стану цієї системи, що розмежовують множину її можливих станів на підмножини, що відповідають інтегральним висновкам про ступінь виконання системою покладених на неї функцій.

Ці підмножини можуть відповідати таким оцінками стану системи:

– забезпечується ефективне функціонування регіональної системи інформаційної безпеки;

– функціонування такої системи є ускладненим;

– функціонування такої системи порушено;

– функціонування такої системи зірвано.

Крім того, перелічені вище стани системи забезпечення інформаційної безпеки можна оцінювати залежно від знаку та розміру зміни таких показників оцінювання її стану:

– відбуваються розвиток системи та зміцнення її положення;

– відбуваються негативні зміни, що знижують значимість системи в забезпеченні регіональної безпеки.

Інакше кажучи, це можуть бути або розвиток, або деградація [2, 14].

У цілому функціонування системи вважається ефективним, якщо воно відповідає описаним нижче значенням окремих показників оцінювання її стану.

1. Забезпечується гарантований захист інформації, яка є державною таємницю, і досить високий рівень захисту тієї, яка належить до службової таємниці. При цьому частка об'єктів захисту, на яких виконуються вимоги, встановлені щодо забезпечення інформаційної безпеки, має становити:

– для об'єктів особливої важливості − не менше 95−99 % залежно від грифу секретності відомостей, що захищаються;

– для інших об'єктів − не менше 90 %.

2. Забезпечується ефективна робота функціональних підсистем забезпечення інформаційної безпеки. Частка обслужених заявок на виконання певного виду робіт від необхідної кількості повинна у цьому разі становити не менше 70−80 % у кожній із функціональних підсистем.

3. Забезпечується ефективне управління цією системою, яке характеризується:

– повнотою розроблення системи документів у розглядуваній сфері і забезпечення цими документами виконавців у ступені не менше 60−70 % за кожним видом документів;

– повнотою формування органів управління в підсистемі управління, об'єктних і функціональних підсистемах − не менше 70−80 % від заданої організаційної структури;

– повнота необхідної інформації про стан елементів системи − не менше 95−99 %;

– повна реалізація програм і планів розвитку відповідної системи − не менше 70−80 %.

Указані критерії є орієнтовними і ґрунтуються на досвіді функціонування складних організаційно-технічних систем (наприклад, систем радіоелектронної боротьби, систем управління бойовими діями). У міру накопичення досвіду оцінювання і статистичного матеріалу по запропонованим показникам оцінювання стану систем забезпечення інформаційної безпеки ці критерії повинні уточнюватися стосовно конкретної регіональної її системи.

Нагадаємо, що стан інформаційної безпеки регіону багато в чому зумовлюється ефективністю використання інформаційних ресурсів усієї нашої держави, її регіонів і муніципальних утворень для соціально-економічного управління регіоном і забезпечення життєдіяльності органів державної влади й місцевого самоврядування, різних підприємств та організацій і окремих осіб [3, с. 57]. З іншого боку, таке використання визначається обраним режимом поширення інформації (доступу до неї) та її захисту.

У разі вільного поширення інформації повністю реалізуються переваги її відкритого використання в різних сферах, але при цьому інтересам певних суб'єктів може бути завдано збитків через те, що найбільш важливі дані стануть передчасно відомі недружнім суб'єктам, причому чим раніше настає етап вільного поширення інформації, тим більшими можуть виявитись розміри такого збитку.

У разі обмеження поширення відомостей позитивним наслідком є запобігання зазначеного вище збитку, натомість при цьому суб'єктам доводиться витрачатися на захист відомостей та упущену вигоду, що залежать від терміну запроваджених обмежень.

Отже, для забезпечення найефективнішого використання інформації за час її життєвого циклу, протягом якого вона є актуальною, необхідно вибрати такий режим її поширення, за якого інтегральний ефект від використання інформації з огляду на співвідношення позитивних і негативних наслідків

досягав би максимальної величини. У разі такого підходу обмеження поширення інформації на певний час є одним із способів управління інформаційним ресурсом власника з метою досягнення максимального інтегрального ефекту від його використання.

При цьому документом, що встановлює обмеження на доступ до інформації, служить перелік відомостей, віднесених до інформації обмеженого доступу (службової, комерційної та інших видів таємниць).

Висновки. Таким чином, нами обґрунтовано, що за своєю будовою державна система інформаційної безпеки є багаторівневою і багатофункціональною системою. До її структури належать державні органи управління системою інформаційної безпеки й територіальні органи виконавчої влади, які вирішують відповідні загальносистемні завдання, та об'єктні (цільові) й функціональні підсистеми державної системи інформаційної безпеки.

Під критеріями оцінювання стану регіональної системи інформаційної безпеки рекомендовано розуміти порогові значення сукупності показників оцінювання стану цієї системи, що розмежовують множину її можливих станів на підмножини, що відповідають інтегральним висновкам про ступінь виконання системою покладених на неї функцій.

Список використаних джерел:

1. Дєгтяр А. О. Державно-управлінські рішення: інформаційно-аналітичне та організаційне забезпечення : монографія. Харків : Вид-во ХарРІ НАДУ «Магістр», 2004. 224 с.

2. Тихомиров О. О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: мета, засоби і методи, принципи, результати. Information Security of the Person, Society and State. 2012. № 3(10). С. 11−17.

3. Шемшученко Ю. С. Правове забезпечення інформаційної діяльності в Україні / за заг. ред. Ю. С. Шемшученка, І. С. Чижа. Київ : Юридична думка, 2011. 384 с.

4. Маращук А. І. Інформаційні ресурси держави: зміст та проблеми захисту [Електронний ресурс] Режим доступу : http://www.ndcpi.org.ua.

References:

1. Diehtiar A. O. Derzhavno-upravlinski rishennia: informatsiino-analitychne ta orhanizatsiine zabezpechennia : monohrafiia. Kharkiv : Vyd-vo KharPI NADU «Mahistr», 2004. 224 c.

2. Tykhomyrov O. O. Diialnisnyi pidkhid u doslidzhenniakh zabezpechennia informatsiinoi bezpeky: meta, zasoby i metody, pryntsypy,

rezultaty. Information Security of the Person, Society and State. 2012. № 3(10). S. 11−17.

3. Shemshuchenko Yu. S. Pravove zabezpechennia informatsiinoi diialnosti v Ukraini / za zah. red. Yu. S. Shemshuchenka, I. S. Chyzha. Kyiv : Yurydychna dumka, 2011. 384 s.

4. Marashchuk A. I. Informatsiini resursy derzhavy: zmist ta problemy zakhystu [Elektronnyi resurs] Rezhym dostupu : http://www.ndcpi.org.ua.