УДК 351 (477)
DOI: 10.35340/2308-104X.2019.84-3-02

СУЧАСНІ ПРИНЦИПИ ТА МЕТОДИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

MODERN PRINCIPLES AND METHODS OF PUBLIC POLICY IN INFORMATION SECURITY

ОРЛОВА Н. С.,
доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування, Київський національний торговельно-економічний університет
ЯРОВОЙ Т. С.,
кандидат наук з державного управління, доцент, доцент кафедри публічного адміністрування Міжрегіональна Академія управління персоналом

ORLOVA N.,
Doctor of Science in Public Administration, Professor, Department of Public Administration and Administration, Kyiv National University of Trade and Economics
YAROVOY T.,
Candidate of Sciences in Public Administration, Associate Professor, Department of Public Administration Interregional Academy of Personnel Management

У статті досліджено основні цілі та принципи політики забезпечення інформаційної безпеки в країні. Узагальнено методологічний апарат забезпечення інформаційної безпеки та визначено рівні інформаційної безпеки. Виділено методи впливу на інформацію. Обґрунтовано, що специфіка методів, що використовуються, залежить від суб'єкта діяльності, об'єкта впливу, переслідуваних цілей. Визначено напрямки вдосконалення державної політики у сфері інформаційної безпеки в Україні.

Ключові слова: *державна політика; інформаційна безпека; інформація; принцип, метод, стратегія.*

В статье исследованы основные цели и принципы политики обеспечения информационной безопасности в стране. Обобщен методологический аппарат обеспечения информационной безопасности и определены уровни информационной безопасности. Выделены методы воздействия на информацию. Обосновано, что специфика используемых методов зависит от субъекта деятельности, объекта воздействия, преследуемых целей. Определены направления совершенствования государственной политики в сфере информационной безопасности в Украине.

Ключевые слова: *государственная политика; информационная безопасность; информация; принцип, метод, стратегия.*

The article explores the main goals and principles of information security policy in the country. The methodological apparatus of information security is generalized and the levels of information security are determined. It is

highlighted methods for influencing information. It is substantiated that the specificity of the methods used depends on the subject of activity, the object of influence, the goals pursued. The directions of improvement of the government policy in the field of information security in Ukraine are determined.

Key words: *public policy; informational security; information; principle, method, strategy.*

Постановка проблеми. Ефективність уряду будь-якої країни залежить від його інформаційного забезпечення. Саме інформація забезпечує оптимальну діяльність державної структури, розвиток масової політичної свідомості, взаємодію суб'єкта та об'єкта державного управління, а інформаційні технології – позитивні соціальні зміни.

Забезпечення інформаційної безпеки – одна з ключових функцій держави, яка формується на основі співставлення небезпек і загроз із наявними ресурсами та вибором відповідної стратегії управління ними.

Розвиток національного інформаційного простору України характеризується негативною тенденцією через нестабільний економічний розвиток та недосконале правове регулювання. Ці умови створюють потенційні та реальні загрози інформаційній безпеці держави та суспільства. За таких умов актуальним постає питання дослідження механізмів державного реагування на сучасні загрози та виклики інформаційній безпеці.

Аналіз останніх досліджень і публікацій. Вивченню різних аспектів забезпечення інформаційної безпеки державою присвячені роботи таких науковців, як Бєлай С. В. [1], Домбровська С. М. [2], Іщенко В. М. [3], Коротич О. Б. [4] та інших. Однак, у вітчизняній і зарубіжній літературі недостатньо розробленими залишаються питання, що пов'язані саме з методологію формування інформаційної безпеки держави в умовах сучасних викликів та загроз. Сьогодні актуалізується необхідність дослідження механізму формування та розвитку інформаційної безпеки країни, що зумовило вибір теми статті.

Мета статті. Головною метою цієї роботи є визначення принципів та методів державної політики в сфері інформаційної безпеки, напрями вдосконалення державної політики для забезпечення національної безпеки країни.

Виклад основного матеріалу дослідження. Державна політика забезпечення інформаційної безпеки України є складовою політики національної безпеки. Вона передбачає системну превентивну діяльність органів влади по наданню гарантій інформаційної безпеки особі, соціальним групам та суспільству в цілому. Політика спрямована на досягнення такого рівня духовного та інтелектуального потенціалів країни, який є достатнім для розвитку її державності і соціального прогресу.

Основними цілями політики забезпечення інформаційної безпеки є:

створення умов для своєчасного виявлення джерел інформаційних загроз та визначення можливих наслідків їх дії;

визначення комплексу превентивних заходів з метою нейтралізації або зменшення (послаблення) негативних наслідків реалізації інформаційних загроз;

створення умов (можливостей) забезпечення своєчасної, повної і точної інформації для прийняття рішень;

удосконалення інформаційної діяльності з метою гармонізації особистих, суспільних і державних інтересів, що є основою досягнення політичної, економічної і соціальної стабільності в суспільстві;

наповнення усіх сфер діяльності знаннями, що становлять інформаційну базу духовного відродження, інтелектуального розвитку, навчання та виховання громадян України;

здійснення ефективного (рівноправного, взаємовигідного) міждержавного інформаційного співробітництва [2].

Основними принципами забезпечення інформаційної безпеки є: принципи забезпечення інформаційної безпеки: пріоритет прав, свобод і законних інтересів людини і громадянина; верховенство права, рівність усіх суб'єктів правовідносин перед законом; відповідальність держави перед людиною за свою діяльність; комплексний підхід до вирішення завдань забезпечення інформаційної безпеки; єдність і взаємозв'язок напрямів забезпечення інформаційної безпеки; розмежування сфер відповідальності й повноважень державних органів і органів місцевого самоврядування з питань забезпечення інформаційної безпеки; участь у міжнародних і регіональних системах інформаційної безпеки; оперативність, своєчасність, превентивність і адекватність заходів щодо попередження і захисту від зовнішніх інформаційних загроз та нейтралізації джерел внутрішніх інформаційних загроз [5].

Перераховані принципи забезпечення інформаційної безпеки є вихідними положеннями формування і функціонування системи інформаційної безпеки як системо-утворюючого фактору всіх складових національної безпеки, норм і правил поведінки громадян, державних і суспільних інститутів України у цій сфері.

Діяльність щодо забезпечення інформаційної безпеки України є, за Конституцією України, однією з найважливіших функцій держави, справою всього українського народу. До основних принципів державної політики в Україні у цій сфері можна віднести такі:

верховенство права юридичних та фізичних осіб, що беруть участь в інформаційній діяльності;

відкритість інформаційного простору (інформаційного середовища) України з урахуванням обмежень, що визначені законами;

централізовано-децентралізоване державне керівництво системою забезпечення інформаційної безпеки;

системний (комплексний) підхід до вирішення проблем забезпечення інформаційної безпеки;

перспективну оцінку досягнутих проміжних результатів у забезпеченні інформаційної безпеки;

зацікавленість «першого керівника» у вирішенні проблем забезпечення інформаційної безпеки;

персональну відповідальність за порушення вимог законодавства у сфері забезпечення інформаційної безпеки [5].

Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності й складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану.

Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

Важливими методами аналізу стану забезпечення інформаційної безпеки є методи опису та класифікації. Для здійснення ефективного захисту системи управління Національною безпекою слід описати та класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу рівня забезпечення інформаційної безпеки використовуються методи дослідження при чинних зв'язків. За допомогою даних методів виявляються причинні зв'язки між загрозами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод розбіжності, метод сполучення схожості і розбіжності, метод супроводжувальних змін, метод залишків.

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту.

Що стосується сфери інформаційної безпеки, то у ній зазвичай виділяють: фізичний; програмно-технічний; управлінський; технологічний; рівень користувача; сітьовий; процедурний (табл. 1) (на основі [2]).

Таблиця 1.

Рівні інформаційної безпеки

Рівень	Характеристика
Фізичний	Здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій.
Програмно-технічний	Здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності
Рівень управління	Здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.
Технологічний	Здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.
Рівень користувача	Реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.
Сітьовий	Політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.
Процедурний	Вживаються заходи, що реалізуються людьми (управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт).

Виділяють декілька типів методів забезпечення інформаційної безпеки:

одноріневі методи будуються на підставі одного принципу управління інформаційною безпекою;

багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких використовується для вирішення

власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;

комплексні методи – багаторівневі технології, які об'єднані у єдину систему координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

інтегровані високоінтелектуальні методи – багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів з організаційним управлінням [2].

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать: прийняття рішення по визначенню області та контексту інформаційної загрози і складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній, соціальній та інших сферах життєдіяльності; забезпечення адекватного сприйняття загрози та небезпеки у нижчих організаційних ланках системи управління національної безпеки; виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи управління: трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну [5].

В сучасних умовах розвитку 58% держав мають національну стратегію інформаційної безпеки (в 2017 році – 50%), 91% держав (177 країн) мають закони, пов'язані із мережевим захистом порівняно з показником минулого року – 79%. На рис. 1. наведено інформацію щодо кількості країн світу, які впроваджують заходи з інформаційної безпеки в практику державного управління, та країн, які не визначають забезпечення інформаційної безпеки ключовим показником ефективності урядових програм.

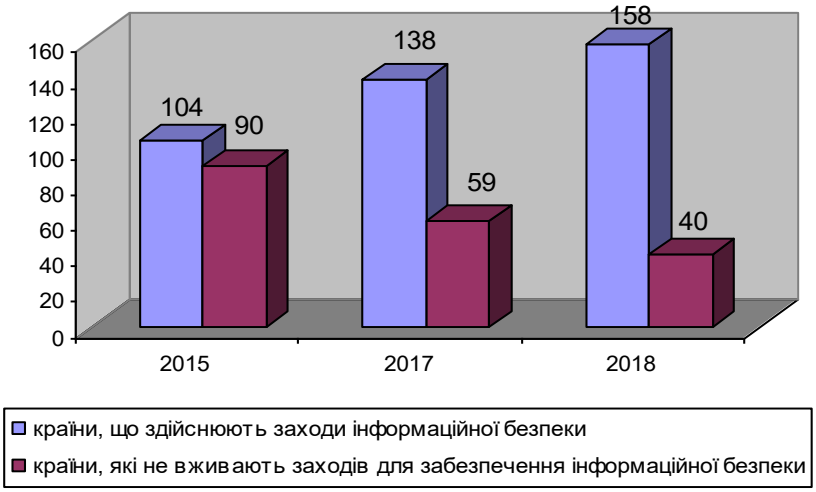

Рис. 1. Країни світу, що впроваджують заходи для забезпечення інформаційної безпеки [6]

Специфіка методів, що використовуються, значно залежить від суб'єкта

діяльності, об'єкта впливу, а також переслідуваних цілей. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю по забезпеченню інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів по нейтралізації інформаційних загроз.

Саме суспільство використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози.

Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. Основним методом аналізу інформаційних ризиків є кількісний та якісний аналіз, факторний аналіз тощо. Метою якісної оцінки ризиків є ранжування інформаційних загроз та небезпек за різними критеріями, система яких дозволить сформувати ефективну систему впливу на них.

Важливим методом забезпечення інформаційної безпеки є також метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний противник паралізує систему державного управління і відповідно знижує здатність підтримувати державне управління в межах оптимальних параметрів [2].

Також можна зазначити метод моделювання, за допомогою якого можна проводити навчання з інформаційної безпеки. Серед методів забезпечення інформаційної безпеки важливе значення відіграє метод дихотомії. Не менш важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформаційної безпеки.

Методи впливу на інформацію у формі повідомлень можна поділити також на електронні та неелектронні. Електронні методи впливу застосовуються у тих випадках, коли повідомлення закріплюються на електромагнітних носіях, котрі призначені для оброблення за допомогою засобів обчислювальної техніки. Вони полягають у знищенні, викривленні, копіюванні повідомлень, які зберігаються на цих пристроях. Неелектронні методи за своєю суттю мають той самий зміст, але реалізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформації [7].

Методи впливу на інформаційну інфраструктуру можуть бути поділені на інформаційні та неінформаційні. Інформаційні методи впливу орієнтовані на порушення формування інформаційно-телекомунікаційних систем, мереж зв'язку, засобів автоматизації управління, систем автоматизованої обробки інформації, і таким чином, на попередження нанесення шкоди предметам суспільних відносин, що захищаються [8].

Таким чином, для протидії загрозам інформаційній безпеці вживаються необхідні заходи як у напряму надання певного впливу на джерело загрози, так і в напряму укріплення об'єкта безпеки.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від різних загроз. В Україні на недостатньому рівні усвідомлюють небезпеку в інформаційній сфері: використовують застарілі підходи та технології; відсутні штатні одиниці в органах державного управління інформаційною безпекою; недостатня підготовка відповідних фахівців для системи управління

національною безпекою. Сучасна державна політика має відповідно реагувати і гарантувати ефективну діяльність у сфері інформаційної безпеки.

Висновки і перспективи подальших досліджень. На основі проведеного дослідження державної політики в сфері інформаційної безпеки доведено, що державна політика в сфері інформаційної безпеки є складовою політики національної безпеки та спрямована на досягнення відповідного рівня духовного та інтелектуального потенціалів країни для розвитку її державності і соціального прогресу. Досліджено основні цілі та принципи політики забезпечення інформаційної безпеки в країні, які є вихідними положеннями формування і функціонування системи інформаційної безпеки.

Узагальнено методологічний апарат забезпечення інформаційної безпеки: однорівневі методи, багаторівневі методи, комплексні методи, інтегровані високоінтелектуальні методи, загальні методи, кількісний та якісний аналіз, факторний аналіз, метод критичних сценаріїв, метод моделювання та ін.

Визначено рівні інформаційної безпеки (фізичний, програмно-технічний, технологічний, сітьовий, процедурний рівні, рівень управління, рівень користувача). Виділено методи впливу на інформацію: електронні та неелектронні, інформаційні та неінформаційні. Обґрунтовано, що специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також переслідуваних цілей.

Завданням сучасної державної політики є відповідне реагування на виявлені інформаційні загрози і гарантувати ефективну діяльність у цій сфері. Система забезпечення інформаційної безпеки має гарантувати доступність і цілісність інформації, її конфіденційність у випадку необхідності. З метою формування оптимальної системи інформаційної безпеки в Україні необхідним є створення законодавчої та нормативної баз; визначення компетенцій органів державної влади та управління; здійснення контролю за діяльністю юридичних та фізичних осіб у сфері забезпечення інформаційної безпеки; фінансова, наукова та матеріально-технічна підтримка юридичних та фізичних осіб, що беруть участь у створенні системи забезпечення інформаційної безпеки; стандартизація, сертифікація та ліцензування діяльності в сфері забезпечення інформаційної безпеки; удосконалення та розвиток державної інформаційної інфраструктури з урахуванням вимог інформаційної безпеки; розробка міжрегіональних, державних та міждержавних програм розвитку системи інформаційної безпеки.

Реалізація зазначених напрямків дозволить підвищити ефективність державної політики з урахуванням інформаційних загроз та небезпеки та забезпечити постійний контроль та моніторинг за всіма автоматизованими процесами управління.

Література:

1. Бєлай С.В. Державні механізми протидії кризовим явищам соціально-економічного характеру. *Держава та регіони*. 2015. № 1. С. 30-33.

2. Домбровська С. М. Механізми інформаційної безпеки як складові державної безпеки України. *Теорія та практика державного управління.* 2015. №1(48). С.1−5.

3. Іщенко В. М. Міжнародний досвід упровадження електронного урядування. *Держава та регіони.* 2012. №4(40). С.26−30.

4. Коротич О. Б. Державне управління регіональним розвитком країни: теоретико-методологічні засади. *Державне будівництво.* 2010. №1. URL: http://www.kbuapa.kharkov.ua/e-book/db/2010-1/doc/1/02.pdf.

5. Про національну безпеку України: Указ Президента України від № 287/2015 від 26.05.2015 URL: https://zakon.rada.gov.ua/laws/show/287/2015?lang=ru.

6. Global Cybersecurity Index 2018. International Telecommunication Union. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

7. Orlova N. S. E-government as a basis for economic development in Ukraine. Ecoforum. 2012. №1(1). URL: http://www.ecoforumjournal.ro/index.php/eco/article/view/11.

8. Орлова Н. С. Перспективи впровадження електронного врядування в Україні. *Економічний розвиток України в контексті впровадження прогресивних інформаційних технологій та систем управління: матеріли II всеукр. наук.-практ. конф*. м. Київ, 25 лютого 2019 р. Київ, 2019. С.150-152

Referenses:

1. Bjelaj S.V. Derzhavni mekhanizmy protydiji kryzovym javyshham socialjno-ekonomichnogho kharakteru. *Derzhava ta reghiony.* 2015. # 1. S. 30-33.

2. Dombrovsjka S. M. Mekhanizmy informacijnoji bezpeky jak skladovi derzhavnoji bezpeky Ukrajiny. *Teorija ta praktyka derzhavnogho upravlinnja.* 2015. #1(48). S.1−5.

3. Ishhenko V. M. Mizhnarodnyj dosvid uprovadzhennja elektronnogho urjaduvannja. *Derzhava ta reghiony.* 2012. #4(40). S.26−30.

4. Korotych O. B. Derzhavne upravlinnja reghionaljnym rozvytkom krajiny: teoretyko-metodologhichni zasady. *Derzhavne budivnyctvo.* 2010. #1. URL: http://www.kbuapa.kharkov.ua/e-book/db/2010-1/doc/1/02.pdf.

5. Pro nacionaljnu bezpeku Ukrajiny: Ukaz Prezydenta Ukrajiny vid # 287/2015 vid 26.05.2015 URL: https://zakon.rada.gov.ua/laws/show/287/2015?lang=ru

6. Global Cybersecurity Index 2018. International Telecommunication Union. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

7. Orlova N. S. E-government as a basis for economic development in Ukraine. *Ecoforum*. 2012. №1(1). URL: http://www.ecoforumjournal.ro/index.php/eco/article/view/11.

8. Orlova N. S. Perspektyvy vprovadzhennja elektronnogho vrjaduvannja v Ukrajini. Ekonomichnyj rozvytok Ukrajiny v konteksti vprovadzhennja proghresyvnykh informacijnykh tekhnologhij ta system upravlinnja: materily II vseukr. nauk.-prakt. konf. m. Kyjiv, 25 ljutogho 2019 r. Kyjiv, 2019. S.150-152.

The main purpose of this work is to determine the principles and methods of public policy in the field of information security, directions for improving public policy to ensure national security of the country.

The government policy in the field of information security is a component of the national security policy and is aimed at achieving the appropriate level of spiritual and

intellectual potential of the country for the development of its statehood and social progress. It is investigated the basic goals and principles of the information security policy in the country, which are the starting points of the formation and functioning of the information security system.

The methodological apparatus of information security is generalized: single-level methods, multi-level methods, complex methods, integrated high-intellectual methods, general methods, quantitative and qualitative analysis, factor analysis, method of critical scenarios, modeling method, etc.

The levels of information security (physical, software, technological, network, procedural, management, user) were determined. Methods of influence on information are distinguished: electronic and non-electronic, informative and non-informative. It is substantiated that the specifics of the methods used depend significantly on the subject of activity, the object of influence, as well as the goals pursued.

The task of modern government policy is to respond appropriately to identified information threats and to guarantee effective activity in this field. The information security system should guarantee the availability and integrity of information, its confidentiality when necessary. In order to create an optimal information security system in Ukraine, it is highlighted directions of public policy in fiekd of information security: to create legislative and regulatory frameworks; determination of competencies of public authorities and management; control over the activity of legal entities and individuals in the field of information security; standardization, certification and licensing of information security activities; development of interregional, government and interstate information security system development programs. Implementation of these directions will allow to increase the effectiveness of the government policy taking into account information threats and dangers and to ensure constant control and monitoring of all automated management processes.