НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

ТОРІЧНИЙ Вадим Олександрович

УДК 351:342.57

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ТРАНСФОРМАЦІЙНИХ ВИКЛИКІВ І ЗАГРОЗ

25.00.05 – державне управління у сфері державної безпеки
та охорони громадського порядку

Подається на здобуття наукового ступеня доктора наук
з державного управління

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ В.О. Торічний

Науковий консультант: ШВЕДУН Вікторія Олександрівна,
доктор наук з державного управління, професор

Харків – 2020

АНОТАЦІЯ

Торічний В. О. Інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів і загроз. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку. Національний університет цивільного захисту України, Харків, 2020.

У дисертації визначено сутність інформаційної політики як феномена інформаційного суспільства і забезпечення його безпеки за допомогою критеріїв систематизації та відповідних їм форм і видів інформаційного забезпечення національної безпеки. Досліджено методологічні основи інформаційного забезпечення державної політики безпеки держави, класифіковано методи оцінки, 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. Проаналізовано процес інформатизації державно-управлінських відносин у формуванні державної безпеки в умовах глобального інформаційного суспільства, здійснено порівняльний аналіз вітчизняного й закордонного досвіду розробки та впровадження інформаційного забезпечення державної безпеки, визначено особливості функціонування організаційно-правових механізмів інформаційного забезпечення державної безпеки, а також охарактеризовано поточний стан і тенденції розвитку державної інформаційної політики в Україні.

Розроблено комплекс заходів з інвентаризації та категорування інформаційних ресурсів у державному та регіональному інформаційному просторі, запропоновано напрями модернізації єдиної державної політики у

сфері інформаційної безпеки, а також сформульовано пропозиції щодо вдосконалення державної системи інформаційної безпеки.

Сформульовано концептуальні положення інформаційного забезпечення державної безпеки, виокремлено стратегічні орієнтири та розроблено пропозиції щодо напрямів трансформації системи інформаційного забезпечення державної безпеки України.

Ключові слова: державне управління, інформаційне забезпечення, національна безпека, державна інформаційна політика, державна система інформаційної безпеки, стратегія державного забезпечення інформаційної безпеки.

ANNOTATION

Torichniy V. O. Information support of state security of Ukraine in conditions of transformational challenges and threats. – The qualified scientific work on the right of manuscript.

Dissertation on competition of Doctor of Sciences degree in Public Administration by specialty 25.00.05 – Public Administration of State Security and Enforcement of Public Order. National University of Civil Defence of Ukraine, Kharkiv, 2020.

The thesis reveals: the essence of information policy as a phenomenon of the information society and ensuring of its security by identifying the systematization criteria and appropriate forms, types, information support of national security. Also the methodological basis of information support of the state security policy is studied, the methods of assessment, receipt and submission of information within implementation of information security of Ukraine are classified, the importance of information security of public-management processes in the context of democratization of society is revealed, the role of state-management institutions as key factors in the implementation of information policy to ensure the national security of modern Ukraine is shown,

the process of informatization of public-management relations in formation of state security in conditions of global information society is analyzed.

In addition, the foreign experience concerning development and implementation of the state security information support are analyzed, the peculiarities of the functioning of organizational and legal mechanisms of the state security information support are highlighted, the current state and trends of development of state information policy in Ukraine ware described.

A set of measures to inventory and categorize the information resources in the state and regional information space is carried out in the work, the directions of modernization of the unified state policy in the field of information security are proposed, the proposals for improvement of the state information security system are formulated.

The conceptual bases of information support of state security are formulared in the work. Besides, the strategic guidelines of information support of state security of Ukraine are identified, the directions of transformation of the system of information support of state security of Ukraine are proposed.

A set of popular scientific and special methods based on modern scientific principles of state-management and related sciences is used in the work in order to achieve the stated goal, to solve the tasks caused by it, and to ensure scientific validity of research and its results.

The methodology of dissertation work is formed with the help of induction and derivation methods, which allowed formulating a hypothesis of the study, as well as building of the heuristic models of information support of state security. The methods of scientific generalization and logical analysis are the basis for determining of the level of development of processes of information support of state security in the scientific literature. The systematic approach is also used in the work - to improve the system of information support of state security. The presence of a comparative method in the study is due to the need to compare domestic and foreign experience concerning development and implementation of state security information support.

The use of a normative and value approach is caused by the need to evaluate and analyze public information policy in terms of its axiological nature and its compliance with functioning and ideal norms and values. The dissertation work also uses the method of structural modeling - to build a model of the State Security Information Support Strategy.

Keywords: public administration, information support, national security, state information policy, state information security system, state information security strategy.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

1. Торічний В. О. Інформаційне забезпечення безпеки держави в умовах інформаційного суспільства: державно-управлінський аспект : монографія. Харків : НУЦЗУ, 2020. 274 с.

2. Торічний В. О. Основні функції та принципи інформаційного забезпечення держави. *Державно-управлінські студії*. 2018. № 8 (10). URL: http://studio.ipk.edu.ua/wp-content/uploads/2019/11/Torichnyy-O.V.-Inform.-zabezp..pdf

3. Торічний В. О. Проблема інформаційної безпеки в умовах розвитку інформаційного суспільства. *Теорія та практика державного управління*. 2019. № 2 (65). С. 256–262.

4. Торічний В. О. Процеси інформатизації державно-управлінських відносин та їх вплив на безпеку держави. *Теорія та практика державного управління.* 2019. № 4 (67). С. 179–187.

5. Торічний В. О. Формування та впровадження державної інформаційної політики як запорука забезпечення державної безпеки. *Вісник Національного університету цивільного захисту України*. 2019. Вип. 1 (10). С. 64–69. (Серія «Державне управління»).

6. Торічний В. О. Особливості державного управління регіональними системами інформаційної безпеки. *Публічне управління і адміністрування в Україні*. 2019. № 11. С. 183–185.

7. Торічний В. О. Особливості побудови державної системи інформаційної безпеки. *Вчені записки Таврійського національного університету ім. В. І. Вернадського*. 2019. Т. 30 (69). № 3. С. 180–182.

8. Торічний В. О. Інформаційне забезпечення державної політики як найважливіший фактор безпеки держави. *Актуальні проблеми державного управління*. 2019. № 1 (55). С. 77–85.

9. Торічний В. О. Технології формування та реалізації інформаційної політики держави. *Вісник Національного університету цивільного захисту України*. 2019. Вип. 2 (11). С. 201–207. (Серія «Державне управління»).

10. Торічний В. О. Дослідження пропаганди як інструменту інформаційного забезпечення державної безпеки. *Право та державне управління*. 2019. № 3 (36). Т. 2. С. 183–186.

11. Торічний В. О. Дослідження методів оцінки результативності державної інформаційної політики у контексті забезпечення державної безпеки. *Держава та регіони*. 2019. № 3 (67). С. 200–203. (Серія «Державне управління»).

12. Торічний В. О. Інформаційне забезпечення безпеки держави в контексті використання комп'ютерних технологій: державно-управлінський аспект. *Актуальні проблеми державного управління*. 2019. № 2 (56). С. 39–46.

13. Торічний В. О. Стратегічні орієнтири інформаційного забезпечення державної безпеки України *Державне управління: удосконалення та розвиток*. 2019. № 11. URL: http://www.dy.nayka.com.ua/?op=1&z=1711

14. Торічний В. О., Шведун В. О. Державний функціональний комплекс забезпечення інформаційної безпеки на прикладі ветеринарного нагляду і контролю. *Публічне управління і адміністрування в Україні*. 2020. Вип. 15. С. 118–121.

Особистий внесок здобувача: *розробка методичного підходу щодо застосування заходів щодо забезпечення інформаційної безпеки у спеціалізованих галузях.*

15. Торічний В. О., Шведун В. О. Державні механізми забезпечення корпоративної інформаційної культури. *Державно-управлінські студії*. 2019. №1(12). URL: http://studio.ipk.edu.ua/wp-content/uploads/2020/02/Borovs-ka-7.pdf

Особистий внесок здобувача: *пропозиція комплексу заходів щодо вдосконалення державних механізмів забезпечення інформаційної культури.*

16. Торічний В. О. Система інформаційного забезпечення державної безпеки України. Державне будівництво. 2020. № 1. URL: www.kbuapa.kharkov.ua/e-book/db/2020-1/index.html

17. Торічний В. О. Умови ефективної розробки та впровадження державної інформаційної політики. *Публічне управління та митне адміністрування.* 2020. № 2 (25). С. 50–62.

Праці, які додатково відображають наукові результати дисертації

18. Торічний В. О. Необхідність створення і розвитку державної системи інформаційної безпеки: впровадження європейського досвіду дослідження впливових факторів. *Актуальні проблеми європейської та євроатлантичної інтеграції України* : матеріали 16-ої регіон. наук.-практ. конф. Дніпро : ДРІДУ НАДУ, 2019. С. 229–230.

19. Торічний В. О. Дослідження суперечностей у системі інформаційного забезпечення державної безпеки соціуму в умовах функціонування цифрового суспільства. *Актуальні проблеми економіки, управління та фінансів* : матеріали міжнар. наук.-практ. конф. Дніпро : Університет митної справи та фінансів, 2019. С. 141–143.

20. Торічний В. О. Формування та реалізація єдиної державної політики у сфері інформаційної безпеки. *Державне управління у сфері цивільного захисту: наука, освіта, практика* : матеріали міжнар. наук.-практ. конф. Харків : Вид-во НУЦЗУ, 2019. С. 112–113.

21. Торічний В. О. Процеси управління інформаційним забезпеченням соціальної безпеки в державі: особливості та вимоги. *Інформаційні технології: наука, техніка, технологія, здоров'я* : тези доповідей XXVII наук.-практ. конф. MicroCAD-2019. Ч. IV. Харків : НТУ «ХПІ», 2019. С. 122.

22. Торічний В. О. Застосування інформаційно-комунікаційних технологій при реалізації освіти протягом життя. *Інноваційні технології розвитку особистісно-професійної компетентності педагогів в умовах*

післядипломної освіти : матеріали ІІІ Всеукр. наук.-практ. інтернет-конф. Суми : Сумський обласний інститут післядипломної педагогічної освіти, 2019. URL: https://drive.google.com/file/d/1kyurQfLDyMbzXusWvuzpKw5Nnanog2Hc/view.

23. Торічний В. О. Інформаційна безпека як чинник функціонування сучасної держави в контексті формування суспільства знань. *Формування громадянської культури в новій українській школі: традиційні та інноваційні практики* : матеріали ІІ Всеукр. наук.-практ. конф. Суми : Сумський обласний інститут післядипломної педагогічної освіти, 2019. С. 254–256.

24. Торічний В. Державне управління у сфері боротьби з комп'ютерними злочинами як напрям забезпечення національної безпеки й охорони громадського порядку. *Забезпечення діяльності складових сектору безпеки і оборони України* : тези міжнар. наук.-практ. конф. Хмельницький : Вид-во НАДПСУ, 2019. С. 574–575.

25. Торічний В.О. Розробка інноваційних методів державного захисту територіального інформаційного простору. Інноваційний розвиток і підвищення рівня спроможності об'єднаних територіальних громад : матеріали науково-практичної конференції за міжнародною участю. Дніпро : ДРІДУ НАДУ, 2019. С. 301–302.

26. Торічний В. О. Критерії та умови ефективності впровадження механізму реалізації державної інформаційної політики. *Державне управління у сфері цивільного захисту: наука, освіта, практика* : матеріали міжнар. наук.-практ. конф. інтернет-конф. Харків : Вид-во НУЦЗУ, 2020. С. 80–81.

27. Торічний В. О. Шляхи підвищення інформаційної безпеки на державному рівні. *Інформаційні технології: наука, техніка, технологія, здоров'я* : тези доп. XXVIII наук.-практ. конф. MicroCAD-2020. Ч. V. Харків : НТУ «ХПІ», 2020. С. 128–129.

Публікації в інших виданнях

28. Торичный, В. А. (2018). Научные основы формирования и реализации государственной политики украины в сфере информационной безопасности. *East Journal of Security Studies*. 3 (1). Retrieved from: http://repositsc.nuczu.edu.ua/bitstream/123456789/10661/1/torichnyiEJSS.pdf.

29. Torichnyi, V. (2019). Information support of the national security of the state in the context of globalization. *East Journal of Security Studies*. 4 (1), 56–66. Retrieved from: https://ejss.nuczu.edu.ua/index.php/ejss/article/view/9.

30. Торичный В. А. Концептуальные основы формирования и реализации государственной политики в сфере информационной безопасности. *Authority and society*. 2019. № 4 (52). С. 343–349.

31. Торичный В. А. Субъектно-объектная составляющая механизма государственного управления в сфере информационной безопасности / В. А. Торичный. *Virtus*. 2020. № 42. С. 193–196.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі інформаційний обмін досяг найвищого рівня інтенсифікації, а обсяг одержуваної інформації, такої, що зберігається, переробляється і передається, на даному етапі розвитку людства знаходиться вже у своєму максимумі. Найбільш розвинені країни світу вступають в якісно новий етап цивілізаційного розвитку – інформаційне суспільство. При цьому кожна держава неминуче має враховувати, що не існує універсальних способів для переходу в інформаційне суспільство, для кожної з них існує «свій» самобутній і конкретний спосіб.

Реалізація даного проекту потребує насамперед наявність державної концепції побудови інформаційного суспільства, де чітко й однозначно мають бути позначені ролі його основних акторів, які забезпечують національну безпеку держави в інформаційному просторі.

До факторів, що визначають актуальність державно-управлінського аналізу інформаційної політики держави, слід віднести такі:

По-перше, багато країн у своєму розвитку цілком закономірно йдуть до інформаційного суспільства, і перешкоди, з якими вони стикаються на цьому шляху, вимагають наукового осмислення й ретельного аналізу. У свою чергу вдосконалення інформаційно-комунікаційних технологій призвело до виникнення глобального інформаційного простору, і всі країни мають інтегруватися в цей процес. Останній носить об’єктивний характер, однак при цьому існують серйозні відмінності у підходах. Так, Західна Європа і США підійшли до нього більш підготовленими й відповідно знаходяться найближче до побудови цілісного інформаційного суспільства. Глобальна інформатизація суспільства об’єктивно й безумовно поступово стає своєрідним базисом усього державно-управлінського, соціально-політичного, економічного і науково-технічного розвитку. Водночас процес інформатизації тісно пов’язаний з процесом демократизації, розвитком громадянського суспільства, здатного впливати на прийняття тих чи інших

державних рішень. В інформаційному суспільстві має переважати інтерактивний тип комунікації, що обумовлює активне ставлення до інформації та організації інформаційного обміну між суб'єктами інформаційного процесу.

По-друге, інформаційна політика, її розробка та реалізація глобально й перманентно виходять сьогодні на передній план всієї державної політики, оскільки від грамотно розробленої концепції інформаційного забезпечення державної політики та її успішної реалізації багато в чому залежить ефективність роботи всіх державних і громадських структур, і зрештою – їх інформаційна безпека. Інформаційна політика виступає тут як найважливіший засіб підтримки публічного діалогу державної влади і громадянського суспільства. Державна влада, на наш погляд, може користуватися довірою громадян тільки в тому випадку, якщо одержувач повідомлення є таким же повноправним учасником комунікації, як і ініціатор повідомлення (в даному випадку – держава), а державні інформаційні служби відмовляться у своїй діяльності від технологій односпрямованого впливу на суспільну свідомість. Державне управління інформаційними процесами перш за все необхідне в питаннях, які зачіпають національні інтереси, і в даному аспекті пряме чи непряме втручання держави є закономірним у діалозі перципієнт – реципієнт.

По-третє, не викликає сумніву, що проблема реалізації інформаційної політики, в силу цілої низки причин, нерозривно пов'язана із забезпеченням державної, а відтак і національної безпеки, тому на сучасному етапі розвитку України необхідний комплексний підхід до їх дослідження.

По-четверте, поряд з цим очевидна необхідність власне державно-управлінського аналізу інформаційної політики та механізму її реалізації, тому що саме в цьому конкретному контексті ціла низка проблем не отримали глибокого відображення, оскільки зазначена тематика є досить новою в науці державного управління.

Сьогодні одним із нагальних завдань державного управління в Україні є вироблення ефективної державної інформаційної політики. Це пов'язано в тому числі з тим, що події останнього часу засвідчили, що інформаційна політика держави ще не повною мірою враховує ті досить серйозні зміни, які відбулися й відбуваються в нашій державно-управлінській і політичної реальності.

Проблеми, пов'язані з інформаційною політикою та її реалізацією, в тому числі в умовах перехідного суспільства, були предметом дослідження багатьох науковців, проте деякі з них залишилися маловивченими. Зокрема, наразі недостатньо розробленими є критерії систематизації видів і форм реалізації інформаційної політики та забезпечення державної й національної безпеки, специфіка функціонування інформаційної політики в умовах відносно слабо розвиненої системи комунікацій і можливості інститутів громадянського суспільства впливати на інформаційну політику держави.

Значний внесок у розвиток знань у сфері інформаційного суспільства зробили такі вчені, як Д. Белл, А. Берг, З. Бжезинський, Д. Блюменау, Е. Брандман, П. Браун, Н. Вінер, М. Кастельс, Б. Ківі, Е. Масуда, Д. Тапскотт, Е. Тоффлер, Ф. Уебстер, Г. Хакен, Ю. Харари, К. Шеннон та ін.

Різним аспектам проблеми інформаційного суспільства та забезпечення національної безпеки присвятили свої праці українські автори, серед яких можна виділити А. Баринова, Е. Буравльова, О. Валевську, О. Власюка, В. Голобуцького, В. Горбуліна, А. Гуза, О. Данільяна, Ю. Древаля, Б. Кормич, В. Костюка, О. Кохановського, О. Крюкова, В. Ліпкана, С. Луценка, Є. Макаренко, А. Марущака, П. Маслянка, Й. Масляну, Г. Почепцова, О. Радченко, Я. Романовського, О. Сенченко, В. Степанова, В. Тертічку та ін.

Питанням інформаційного забезпечення національної безпеки держави присвятили свої дослідження багато авторів на пострадянському просторі, серед яких можна виділити О. Андронова, Є. Горєлова, І. Дмітрачкова, Д. Іванова, Г. Іващенко, Н. Лапіна, В. Легасова, А. Манойло, О. Музику,

Г. Мухіна, Ю. Нісневіча, І. Панаріна, Б. Порфирьева, Л. Сморгунова, В. Халіпова, А. Федорова та ін.

Також окремі аспекти забезпечення національної безпеки розглядали у своїх роботах такі вітчизняні вчені, як: У. Бережницька, З. Варналій, А. Возженіков, А. Васильєв, В. Геєць, Р. Дацків, А. Качинський, В. Коврегін, В. Мамонова, Р. Науменко, В. Пономаренко, С. Степашин, О. Судакова, С. Тоцький, Ю. Холтунцов, Т. Шуберт, А. Фоміна, І. Яремко та ін.

Питанням державного управління національною безпекою присвячені численні праці вітчизняних і зарубіжних науковців, зокрема, таких, як: О. Береза, Д. Венцковський, В. Колокольцев, М. Криштанович, Я. Малик, В. Манілов, С. Павленко, С. Пирожков, І. Проценко, І. Руснак, Ш. Султанов, О. Соснін, М. Сунгуровський, та ін.

Проте ступінь дослідження проблеми державного управління національною безпекою наразі залишається недостатньо розкритим, наукові праці з цієї проблематики розрізнені, методологічно необ’єднані, у них відсутня єдина цілісна наукова державно-управлінська теорія.

Науково-теоретичним підґрунтям дисертаційної роботи стали праці вітчизняних і зарубіжних учених, присвячені концептуальним засадам державного управління (В. Авер’янов, В. Бакуменко, О. Бойко-Бойчук, В. Голуб, В. Дзюндзюк, А. Дєгтяр, С. Домбровська, О. Іваницька, О. Кілієвич, В. Князєв, А. Мерзляк, О. Мордвінов, Н. Нижник, В. Олуйко, Ю. Сурмін та ін.), проблематиці інформаційного забезпечення (П. Бакут, О. Дубас, М. Кастельс), державним інформаційним ресурсам (О. Нестеренко, О. Рубанець, О. Сенченко, Г. Сілкова, В. Яковенко), державній інформаційній політиці (І. Арістова, В. Гусєв, О. Карпенко, В. Конах, О. Манойло), загальним питанням інформаційної безпеки (Ю. Борсуковський, А. Гуз, Б. Кормич, Н. Кунанець, С. Ленков, І. Маракова, А. Момот), правовим аспектам інформаційного забезпечення державної безпеки (С. Бондаренко, К. Бєляков, В. Бутузов, А. Венгеров, С. Головань, В. Дурдинець, Л. Харченко) та ін.

У той же час категорії, закономірності, принципи, методи, концепції, моделі, системи, класифікація у сфері інформаційного забезпечення державної безпеки практично не розроблені. Сучасні дослідники зосереджують увагу переважно на окремих проблемах, а питання перетворення України на ефективну державу з точки зору інформаційної безпеки ще не стало предметом всебічного науково-практичного вивчення, що, у свою чергу, потрібує системного аналізу ролі та місця інформаційного забезпечення державної безпеки України в державному управлінні інформаційною безпекою як частини забезпечення національної безпеки.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано у Національному університеті цивільного захисту України відповідно до тематики науково-дослідних робіт «Розробка наукових основ державного управління в сфері безпеки ринку соціально-економічних послуг України з точки зору цивільного захисту» (державний реєстраційний номер 0115U002035), у межах якої дисертантом запропоновано шляхи вдосконалення єдиної державної політики у сфері забезпечення інформаційної безпеки та «Розробка механізмів державного управління соціально-економічною сферою та її галузями в контексті забезпечення безпеки українського суспільства» (ДР № 0118U001007), у межах якої автором вдосконалено систему інформаційного забезпечення державної безпеки в Україні.

Мета і завдання дослідження. *Метою* дисертаційної роботи є розробка теоретико-методологічних засад державно-управлінського аналізу сутності та особливостей реалізації інформаційного забезпечення як фактора національної безпеки сучасної України

Відповідно до поставленої мети визначено такі основні *завдання*:

– розкрити сутність інформаційної політики як феномена інформаційного суспільства та забезпечення його безпеки, визначити основні ознаки інформаційного суспільства за допомогою виявлення критеріїв

систематизації та відповідних їм форм і видів інформаційного забезпечення національної безпеки;

– дослідити методологічні основи інформаційного забезпечення державної політики безпеки держави, структуру національної безпеки, класифікувати інформаційні зв’язки суб'єктів національної безпеки, а також чинники отримання і подачі інформації у забезпеченні інформаційної безпеки України;

– розкрити значення інформаційної безпеки в державно-управлінських відносинах через організацію та здійснення певних принципів інформаційного забезпечення національної безпеки, показати комунікативну взаємодію органів влади та суспільства як ключових суб’єктів реалізації інформаційної політики забезпечення національної безпеки сучасної України;

– проаналізувати процес інформатизації державно-управлінських відносин у формуванні державної безпеки в умовах глобального інформаційного суспільства;

– здійснити порівняльний аналіз вітчизняного та закордонного досвіду розробки та впровадження інформаційного забезпечення державної безпеки;

– охарактеризувати особливості функціонування організаційно-правового механізму інформаційного забезпечення державної безпеки;

– визначити напрями модернізації єдиної державної політики у сфері інформаційної безпеки;

– запропонувати шляхи вдосконалення державної системи інформаційної безпеки;

– сформулювати концептуальні положення інформаційного забезпечення державної безпеки;

– окреслити стратегічні орієнтири інформаційного забезпечення державної безпеки України.

Об’єктом дослідження державна безпека в умовах трансформаційних викликів і загроз.

Предмет дослідження – інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів і загроз.

Методи дослідження. Для досягнення поставленої мети й вирішення зумовлених нею завдань, забезпечення наукової обґрунтованості дослідження і його результатів було використано комплекс загальнонаукових і спеціальних методів, що ґрунтуються на сучасних наукових засадах державно-управлінської та споріднених із нею наук.

За допомогою методів індукції та дедукції сформовано методологію дисертаційної роботи, що дозволило сформулювати гіпотезу дослідження, а також побудувати евристичні моделі інформаційного забезпечення державної безпеки. Основою для визначення рівня розробленості в науковій літературі процесів інформаційного забезпечення державної безпеки стали методи наукового узагальнення та логічного аналізу. Для вдосконалення системи інформаційного забезпечення державної безпеки у роботі застосовано системний підхід. Присутність у дослідженні порівняльного методу зумовлено необхідністю порівняння вітчизняного та закордонного досвіду розробки й упровадження інформаційного забезпечення державної безпеки.

Нормативно-ціннісний підхід використано для оцінки й аналізу державної інформаційної політики з точки зору її аксіологічної сутності, відповідності функціонуючим та ідеальним нормам і цінностям. У роботі також застосовано метод структурного моделювання для побудови моделі Стратегії інформаційного забезпечення державної безпеки.

В основу методології дослідження покладено системний підхід, методологічна специфіка якого визначається тим, що він орієнтує дослідження на розкриття цілісності об’єкта і механізмів, які її забезпечують, виділення різноманітних типів зв’язків складного об’єкта і зведення їх в єдину теоретичну картину. Зокрема, для більш точного вимірювання й оцінювання процесів формування та взаємного впливу систем інформаційної безпеки й розвитку державної політики України у

сфері інформаційної політики застосовано соціологічний метод. З використанням статистичного методу визначено реальний стан досліджуваного об'єкта, а прогностичного – складові функціонально-цільової моделі державного управління інформаційною безпекою країни. Теоретико-концептуальний метод визначив напрям дослідження, втілений в аналізі функцій, структури та параметрів об'єкта, дав змогу запропонувати стратегічні напрями вдосконалення механізмів державного управління інформаційною політикою як важливої складової національної безпеки України. Нормативно-інформаційну базу дисертації склали закони України, укази Президента України, постанови Кабінету Міністрів України, нормативні документи органів державної влади України, Міністерства освіти і науки України, матеріали анкетування, результати особистих напрацювань автора, а також зарубіжні й вітчизняні наукові джерела з досліджуваної проблематики.

Наукова новизна отриманих результатів полягає в розв'язанні актуальної наукової проблеми в галузі науки державного управління з теоретико-методологічного обґрунтування та розробки практичних рекомендацій щодо розвитку процесів інформаційного забезпечення безпеки держави.

При цьому наукова новизна конкретизується в таких положеннях:

уперше:

– сформульовано наукову концепцію інформаційного забезпечення державної безпеки, суть якої полягає, з одного боку, у необхідності глобальної інформатизації сучасного українського суспільства з точки зору інформаційного забезпечення державної безпеки, а також її аналізу як державно-управлінської складової національної безпеки, а з іншого боку − як феномена інформаційного забезпечення державної безпеки, який функціонує в умовах глобального переходу більшості держав світу до управління інформаційним суспільством в умовах швидко мінливого світу з точки зору нових загроз і викликів сучасній політиці державної безпеки;

– визначено критерії систематизації і відповідні форми, види і напрями інформаційної політики сучасних держав щодо забезпечення інформаційної безпеки, де в якості основ класифікації методологічного апарату дослідження інформаційної політики інформаційна безпека розглядається як з позиції її пізнання, так і з позиції впливу на формування ефективної державної політики з урахуванням специфіки функціонування даних методів на перехідному етапі розвитку українського суспільства;

удосконалено:

– методологічний апарат, адаптований до проблеми управління інформаційним забезпеченням безпеки держави, що включає елементи інституційного підходу, а також теорії організації й управління через системно-діалектичну модель проблеми забезпечення безпеки глобального управління, яка розкриває основні суперечності між фактичним станом системи й її цільовим інформаційним станом, якого необхідно досягти за певний час і з найменшими ресурсними витратами;

– положення про те, що проблема забезпечення інформаційної безпеки є проблемою розвитку інформаційного суспільства та докорінно відрізняється від проблеми функціонування держави в постіндустріальний період, маючи на увазі мотиваційну модель поведінки людини через потреби згідно основних циклів управління;

– положення про сутнісний взаємозв'язок світового глобального процесу і процесу забезпечення інформаційної безпеки у вигляді теоретичних аспектів щодо шляхів підвищення цільової ефективності державного управління інформаційним забезпеченням державної безпеки за допомогою розробки і реалізації державної інформаційної політики, яка відповідає сучасним викликам, що стоять перед державою в системі інформаційної безпеки, стосовно її формалізації на відповідній нормативно-правовій базі;

– формалізація теоретико-методологічних розробок та концептуально-конструктивних рішень щодо проблем державного управління

інформаційною безпекою на рівні основних моделей управління через використання у сфері національної безпеки найрізноманітніших інформаційних потоків, а також вивчення та оптимізацію цих потоків в контексті удосконалення інформаційного забезпечення національної безпеки;

дістали подальшого розвитку:

– теоретичний підхід до формування стратегії інформаційного забезпечення державної безпеки, який орієнтований на передбачення умов для створення можливостей максимального впровадження інтелектуальних систем в основні галузі економіки з метою побудови більш відкритої, доступної та конкурентоспроможної економіки через створення єдиного інформаційно-аналітичного середовища державних органів як основного інструменту узгодженого проведення всіх видів реформ державного управління у сфері інформаційної безпеки;

– методологічний підхід до розробки концепції інформаційного забезпечення державної безпеки, яка покликана забезпечити єдність підходів до формування та реалізації єдиної державної політики забезпечення інформаційної безпеки, складає методологічну основу для вдосконалення нормативно-правових актів, що регулюють дану сферу, а також є базисом для створення державної системи забезпечення інформаційної безпеки, яка гарантує захист національних інтересів України в інформаційній сфері яка уможливлює її рівноправну участь у світових інформаційних відносинах, забезпечення надійності та стійкості функціонування критично важливих інформаційних систем, стабільне функціонування й надійний захист єдиного національного інформаційного простору;

– практичний підхід до підвищення ефективності роботи державних органів через автоматизацію їх діяльності, який, на відміну від існуючих, передбачає створення інформаційно-комунікаційної архітектури для кожного державного органу у сфері забезпечення інформаційної безпеки та являє собою сукупність документів і моделей, що містять детальний опис

поточного й перспективного стану державного органу, а також плану заходів з оптимізації взаємозалежностей і взаємозв'язків між функціями, бізнес-процесами, даними, інформаційними системами та компонентами технічної інфраструктури у межах плану інформатизації для забезпечення реалізації стратегічних цілей і завдань державного органу;

– уточнення сутності дефініцій: «інформаційне забезпечення державної безпеки України» як здійснення взаємопов'язаних заходів правового, організаційного, оперативно-розшукового, розвідувального, контррозвідувального, науково-технічного, інформаційно-аналітичного, кадрового, економічного та іншого характеру з виявлення, прогнозування, запобігання, стримування і нейтралізації інформаційних загроз та ліквідації наслідків їх прояву для державної безпеки України; «єдина державна політика інформаційного забезпечення державної безпеки України» як механізм узгодження інтересів суб'єктів інформаційних відносин і знаходження компромісних рішень щодо забезпечення державної безпеки через розробку та реалізацію єдиних стандартів у сфері забезпечення вимог інформаційної безпеки до державних і недержавних інформаційних систем, ресурсів та підтримуючої інфраструктури; «механізм реалізації політики інформаційного забезпечення державної безпеки» як єдиний алгоритм міжвідомчої взаємодії, що виключає дублювання функцій і бере до уваги інформаційну роботу держави в період значущих подій у житті країни через пряму взаємодію державних органів з аудиторією ЗМІ, включаючи технології краудсорсингу, з метою захисту національних інтересів.

Практичне значення отриманих результатів дослідження полягає в можливості й доцільності застосування ключових положень і висновків дисертації в навчальному процесі для розробки та підготовки навчально-методичної літератури, а також у практичній діяльності органів державної влади та органів місцевого самоврядування з метою формування та впровадження державно-управлінських рішень з інформаційного забезпечення державної безпеки.

Пропозиції дисертаційного дослідження використано в роботі Головного управління Державної служби України з надзвичайних ситуацій у Хмельницькій області стосовно створення можливостей максимального впровадження інтелектуальних систем в у процеси забезпечення державної безпеки (довідка № 01-1985/02 від 19.12.2019), виконавчого комітету Хмельницької міської ради щодо формування інформаційно-комунікаційної архітектури органів місцевого самоврядування (довідка № 02-21-598 від 13.05.2020) та департаменту освіти і науки Хмельницької обласної державної адміністрації відносно впровадження елементів запропонованої національної Стратегії інформаційного забезпечення державної безпеки у контексті консолідації всіх верств суспільства для досягнення поставлених цілей інформаційного й інноваційного розвитку (довідка № 1189-41/2020 від 13.05.2020).

Крім того, теоретичні положення та наукові результати дисертаційної роботи використано в навчальному процесі Національної академії Державної прикордонної служби України імені Богдана Хмельницького відносно поглиблення змістовно-понятійної бази щодо інформаційного забезпечення державної безпеки, удосконалення його механізмів, виокремлення принципів функціонування державної системи інформаційної безпеки, а також розвитку єдиної державної політики у сфері інформаційної безпеки в Україні (Акт № 186/20-354 від 17.01.2020).

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею. Всі сформульовані в ній висновки, наукові положення та пропозиції ґрунтуються на особистих дослідженнях здобувача.

Апробація матеріалів дисертації. Основні теоретичні й практичні положення, висновки, пропозиції та рекомендації, сформульовані в дисертації, оприлюднені на таких регіональних і міжнародних науково-практичних конференціях, конгресах і семінарах: «Актуальні проблеми економіки, управління та фінансів» (м. Дніпро, 19 квітня 2019 р.); «Актуальні проблеми європейської та євроатлантичної інтеграції України» (м.

Дніпро, 16 травня 2019 р.); «Державне управління у сфері цивільного захисту: наука, освіта, практика» (м. Харків, 17–18 травня 2019 р., 18–19 березня 2020 р.); «XXVII науково-практичної конференції MicroCAD-2019» (м. Харків, 15–17 травня 2019 р.), «Інноваційні технології розвитку особистісно-професійної компетентності педагогів в умовах післядипломної освіти» (м. Суми, 23 травня 2019 р.); «Формування громадянської культури в новій українській школі: традиційні та інноваційні практики» (м. Суми, 6–7 червня 2019 р.); «Забезпечення діяльності складових сектору безпеки і оборони України» (м. Хмельницький, 22 листопада 2019 р.); «XXVIII науково-практичної конференції MicroCAD-2020» (м. Харків, травень, 2020 р.).

Публікації. Основні положення та отримані наукові результати дисертаційного дослідження відображено в 31 наукових працях, з яких: 1 − одноосібна монографія, 16 статей у вітчизняних наукових фахових виданнях, 4 статті у зарубіжних спеціалізованих виданнях та 10 тез доповідей. Загальний обсяг публікацій за темою дослідження становить 34,6 авт. арк.

Структура та обсяг дисертації обумовлені предметом, метою та завданнями дослідження. Робота складається зі вступу, п’яти розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації становить 375 сторінок, з яких основного тексту – 330 сторінок, кількість використаних джерел – 370 найменувань на 45 сторінках, 6 рисунків і 9 таблиць, 1 додаток – на 5 сторінках.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНИЙ АНАЛІЗ ПРОБЛЕМ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ ТА ЗАГРОЗ

1.1. Інформаційна складова в системі забезпечення державної безпеки

Актуальність цієї проблематики визначається, на наш погляд, всезростаючою роллю інформаційної сфери, а також системи регулювання суспільних відносин, які через це виникають. Під інформаційною сферою мається на увазі сукупність інформації, інформаційної інфраструктури та суб'єктів, що збирають, формують, поширюють і використовують інформацію. Згадана сфера є одним з найголовніших системоутворюючих чинників суспільного життя, що чинить істотний вплив на стан усіх складових сучасної державної безпеки: політичну, економічну, державно-управлінську тощо; при цьому вона значною мірою залежить від інформаційного забезпечення безпеки, і в процесі технічного прогресу ця залежність зростає дедалі сильніше.

Крім того, в сучасних умовах підвищується і роль інформації в розвитку державно-управлінських процесів і як наслідок – збільшуються інформаційні загрози безпеці особи, суспільства та держави. У цьому сенсі останні відіграють роль об'єктів і суб'єктів інформаційної безпеки на таких масштабних рівнях суспільного життя, як регіональний, національно-державний і міждержавний.

Проблеми та пов'язані з інформаційним забезпеченням безпеки держави питання (зокрема щодо шляхів цього забезпечення) не є новими для дослідників – їх постійно порушують у своїх роботах вітчизняні та зарубіжні автори з різними науковими інтересами, які можуть стосуватися цієї теми як прямо, так і опосередковано. Зокрема, різні аспекти забезпечення нацбезпеки

досліджувались у наукових працях А. Васильєва, Н. Віннера, А. Возженікова, І. Панаріна, Г. Почепцова, В. Степанова, С. Чукут, Т. Шуберта, А. Фоміна та ін. Водночас, на наш погляд, питання співвідношення інформаційних аспектів у формуванні національної безпеки сучасних держав у контексті державно-управлінської проблематики наразі не знайшли достатнього висвітлення в науковій літературі.

З огляду на це метою першого підрозділу нашого дослідження є аналіз проблеми інформаційного забезпечення безпеки держави як найважливішої складової національної безпеки в умовах глобалізаційних процесів, що активно відбуваються у світі.

У сучасних умовах інформація є без перебільшення одним із найзначніших ресурсів розвитку цивілізації. Вона активно впливає на всі аспекти життя як окремих суспільств і держав, так і всієї світової спільноти [21]. Однак, як показав досвід, інформація може використовуватись не тільки на благо, але й на шкоду інтересам особи, суспільства та держави.

Розвиток інформаційно-комунікаційних технологій, їх розповсюдження та проникнення практично в усі сфери життєдіяльності людини стає важливим чинником світової інтеграції, соціального розвитку та економічного зростання. Водночас, будучи найсильнішим каталізатором інформаційного обміну, ці технології містять у собі безліч як явних, так і прихованих загроз. Через це надзвичайної актуальності набувають питання забезпечення інформаційної безпеки, яка, у свою чергу, є однією з найголовніших складових нацбезпеки. Крім того, існує думка, що в постіндустріальному світі, де саме інформація не лише стала головним продуктом, а і почала визначальним чином впливати на ухвалення тактичних і стратегічних рішень на рівні державного управління, саме цей різновид безпеки виступає підґрунтям і запорукою національної безпеки держави [321].

Отже, національна безпека у сучасному світі значною мірою залежить від забезпечення інформаційної безпеки, що надає можливість припустити, що з розвитком технічного прогресу ця залежність лише зростатиме [179].

Попри значну увагу, яку науковці, що досліджують проблеми інформаційного суспільства, приділяють питанням забезпечення інформаційної безпеки цього суспільства та держави разом з питаннями розроблення засад і реалізації державної політики в цій галузі, чимало аспектів наразі залишаються мало розробленими, що значно ускладнює розбудову дієвої та ефективної системи забезпечення інформаційної безпеки Української держави.

Останніми десятиліттями інформаційний аспект розвитку суспільства був об'єктом досліджень як зарубіжних, так і вітчизняних науковців. Зокрема, основні аспекти інформаційного суспільства висвітлено в класичних працях західних дослідників Н. Вінера [53; 54], М. Кастельса [134] і Д. Тапскота [270] та ін. Істотний внесок у дослідження питань, що стосується інформаційних аспектів у розвитку суспільства, зробили Д. Белл [338], Г. Хакен [306] та інші вчені. Глобальні проблеми інформаційного розвитку розглядались у роботах вітчизняних дослідників, таких як О. Панарін [222; 223], Г. Почепцов [238], С. Луценко [175], С. Чукут [237] та ін. Проте, попри це, проблему інформаційної безпеки нашої держави досліджено ще не повною мірою.

Виходячи з вищевикладеного, метою нашого дослідження є проведення державно-управлінського аналізу ролі інформаційної безпеки в розвитку інформаційного суспільства за наявності глобалізаційних викликів сучасності.

Сутність терміна «інформаційна безпека» як у науковій літературі, так і в нормативно-правових державних документах трактується не зовсім чітко. На нашу думку, наразі воно є результатом інтеграції змісту понять «національна безпека» та «безпека інформації» [126].

Так, під інформаційною безпекою, як правило, розуміють наявність захисту інформації та потрібної для її підтримки інфраструктури від випадкових чи цілеспрямованих впливів природного або штучного походження, які можуть заподіяти неприйнятну шкоду суб'єктам інформаційних відносин, серед іншого власникам і користувачам інформації та згаданій вище її підтримуючій інфраструктурі.

Під захистом інформації розуміється комплекс заходів, покликаних забезпечувати інформаційну безпеку. На нашу думку, найбільш методологічно адекватним підходом до вирішення проблем інформаційної безпеки є той, відповідно до якого все має починатись з визначення суб'єктів інформаційних відносин та з'ясування їхніх пов'язаних з використанням інформаційно-комунікаційних технологій інтересів, адже загрози інформаційній безпеці фактично є зворотним боком користування згаданими технологіями.

Розуміння і тлумачення сутності пов'язаних з інформаційною безпекою проблем із боку різних категорій суб'єктів держуправління можуть суттєво відрізнятися, втім, загалом у спектрі інтересів суб'єктів, що стосуються застосування інформаційно-комунікаційних технологій, можна виділити такі їх основні категорії, як забезпечення доступності інформації, її цілісності та конфіденційності, а також згаданої вище її інфраструктури. Метою заходів у сфері інформаційної безпеки є захист інтересів зазначених вище суб'єктів інформаційних відносин. Ці інтереси можуть бути дуже різними, але всі їх можна згрупувати навколо таких трьох основних характеристик, як уже згадані доступність, цілісність і конфіденційність. З огляду на це і саму інформаційну безпеку можна тлумачити як відсутність недопустимого ризику, пов'язаного із можливим заподіянням прямої або непрямої (серед іншого майнової та фінансової) шкоди підприємству чи фізичній особі, викликаної порушенням конфіденційності, цілісності та/або доступності інформації.

За основними сферами прояву системне вираження інформаційної безпеки локалізується: а) у сфері функціонування органів держуправління (державна інформаційна безпека); б) у сфері громадянського суспільства (у цьому разі йдеться про інформаційну безпеку суспільства); в) у сфері інтересів особи [181, с. 18; 182].

Говорячи про сутність і внутрішню будову (або структуру) інформаційної безпеки, слід ураховувати, що категорія «інформаційна безпека» на цьому етапі може набувати різних значень у разі використання в різних контекстах. Так, в державних управлінських органах склалися два напрями щодо визначення самого поняття інформаційної безпеки та щодо її структури (будови). У першому (так званому гуманітарному) напрямі інформаційна безпека пов'язується виключно з інститутом державної таємниці. У другому, презентованому головним чином представниками силових структур, домінує протилежна тенденція – розглядуване поняття намагаються поширити фактично на всі можливі відносини в інформаційній сфері, фактично ототожнюючи цей різновид безпеки з останньою [50]. На наш погляд, обидві точки зору являють собою крайнощі.

Якщо повернутись до зв'язку розглядуваної сфери з інтересами, то під інтересами особи в цьому разі доречно мати на увазі, по-перше, її конституційні права на доступ до інформації, по-друге, використання інформації з метою власного фізичного, духовного й інтелектуального розвитку, а також здійснення будь-якої діяльності, не забороненої законом, і по-третє, захист тієї інформації, яка забезпечує безпеку такої особи. Коли йдеться про інтереси суспільства в цій сфері, то розуміється насамперед задоволення згаданих вище інтересів особи у розглядуваній сфері, а також зміцнення демократії в Україні та подальша розбудова правової соціальної держави. Інтереси держави у цій сфері визначаються створенням належних умов для подальшої розбудови вітчизняної інформаційної інфраструктури, забезпечення реалізації пов'язаних з отриманням інформації та користуванням нею конституційних прав і свобод людини та громадянина,

що, у свою чергу, сприятиме зміцненню конституційного ладу, суверенітету і територіальної цілісності України, підвищенню стабільності у політичній, економічній, соціальній, державно-управлінській та інших сферах життєдіяльності, а також зміцненню законності та правопорядку й розвитку рівноправного міжнародного співробітництва на взаємовигідних умовах.

Однією з важливих характеристик інформаційної безпеки суспільства і держави є ступінь їх захищеності, тобто фактично стійкість усіх головних сфер життєдіяльності (як-то економіка, наука, технології, державне управління тощо) до всіх небезпечних, зокрема дестабілізуючих і деструктивних інформаційних впливів, що зачіпають інтереси країни, незалежно від того, здійснюються вони у вигляді впровадження (підкидання) чи навпаки, вилучення інформації. На нашу думку, інформаційна безпека в цьому випадку визначальним чином зумовлюється спроможністю убезпечити державу і суспільство від цих впливів, зокрема їх нейтралізувати. Об’єктами небезпечного інформаційного впливу й, отже, розглядуваної безпеки, виступають людські свідомість і психіка й різноманітні інформаційно-технічні системи будь-якого масштабу чи призначення. Безпосередньо до соціальних об’єктів цієї безпеки належать особа, групи людей (спільноти), суспільство та держава.

Під суб’єктами інформаційної безпеки розглядаються ті органи і структури, які займаються її забезпеченням. До них належать органи як виконавчої, так і законодавчої та/або судової влади.

У науковій літературі поняття «інформаційна безпека» тривалий час зводили до поняття «безпека інформації», згодом виникла інша тенденція – на додаток до цього (або замість цього) деякі автори почали підміняти його поняттям «захищеність суб’єктів інформаційних відносин від негативних інформаційних впливів».

Втім, наявність певних нюансів у різних визначеннях не змінює основної суті згаданих вище основних підходів. Вважаємо це розуміння

поняття «інформаційна безпека» недостатньо повним і таким, що потребує уточнення.

На нашу думку, визначення цього терміна методологічно має ґрунтуватися на розумінні того, що категорія «безпека» стосується не власне інформації як такої (хоча інформаційна безпека нерідко торкається і її теж), а насамперед суб'єктів інформаційного середовища, тобто залучених в інформаційний процес фізичних і юридичних осіб. Із практичної точки зору можна стверджувати, що ця безпека без суб'єкта інформаційного середовища взагалі не існує, натомість саме цей суб'єкт зумовлює її показники.

Ми вважаємо, що забезпечення безпеки в аспекті врахування інтересів суб'єкта інформаційних відносин є процес формування сприятливих умов діяльності, цілеспрямоване створення (отримання, пошук) умов, за яких реалізовуватимуться його інтереси й досягатимуться поставлені ним цілі.

При цьому найважливішою основою цілеспрямованої діяльності у сфері згаданих відносин є цінності їх учасників. Стосовно суб'єкта забезпечення безпеки є процесом оволодіння ним необхідними умовами власного існування. Це, у свою чергу, означає, що безпека передбачає забезпечення наявності таких умов, коли суб'єкти щонайменше зберігають і відтворюють свої цінності.

Як справедливо вважає Г. Іващенко, забезпечення безпеки як процес оволодіння умовами існування, водночас є процесом реалізації свободи суб'єкта як здатності контролювати умови власного існування. На його думку, свобода і безпека – явища, тісно пов'язані між собою, що утворюють фундаментальні аспекти соціального буття, найважливіші характеристики соціальних суб'єктів [120, с. 52].

Отже, під інтересами суспільства у розглядуваній сфері слід розуміти захист життєво важливих інтересів особи в цій само сфері, а також можливість реалізовувати конституційні права і свободи людини та громадянина для зміцнення демократії, досягнення громадського злагоди та її підтримання і підвищення творчої активності населення, а під інтересами

держави – забезпечення умов для подальшої розбудови інформаційної інфраструктури країни, реалізації згаданих вище конституційних прав і свобод із метою зміцнення конституційного ладу, суверенітету і територіальної цілісності держави [346].

Сучасний перебіг подій неможливо повною мірою усвідомити без урахування глобалізаційних викликів, які суттєво зачіпають і інформаційну сферу. У цьому сенсі глобалізація стала найважливішою тенденцією світового розвитку кінця XX – початку XXI ст. Ця тенденція чітко проявляється в економічній, соціальній, державно-управлінській, ідеологічній та культурній сферах.

Останніми роками в цьому ряду на передній план висувається інформаційна сфера, яка через стрімкий розвиток інформаційно-комунікаційних технологій і появу принципово нових і високоефективних методів інформаційного обміну та впливу стає важливим інструментом соціально-економічних і політичних перетворень. Як справедливо зазначав відомий американський футуролог О. Тоффлер, на сучасному етапі знання та інформація стали найважливішими ресурсами влади [304, с. 46].

У сучасному світі відбуваються інтенсивне нарощування інформаційно-комунікаційного потенціалу, інформаційна глобалізація сприяє інтеграційним процесам у всіх інших сферах. Засобами для цього є розвиток комунікацій, використання космічного простору для передачі інформації, зростання глобальних інформаційних мереж, комп’ютеризація багатьох процесів життєдіяльності людства [339].

Нині, попри широке розповсюдження застосування до всіх цих явищ терміна «інформаційне суспільство», експерти не дійшли одностайності у розумінні змісту цього поняття. На думку деяких, під ним слід розуміти суспільство, де забезпечено легкий і вільний доступ до інформації в усьому світі, а з точки зору інших, йдеться про суспільство, де основними об’єктами праці більшості та водночас її результатами є суто інформаційні продукти, такі як безпосередньо сама інформація чи знання. Найбільшу підтримку

серед дослідників отримало визначення інформаційного суспільства як суспільства, за яким головним предметом праці більшості населення є інформація і знання, а знаряддям цієї праці – інформаційні технології.

Більш розгорнуто інформаційне суспільство можна охарактеризувати як особливу фазу розвитку сучасної цивілізації, для якої є типовим різке підвищення значущості інформації і знань для життєдіяльності суспільства, збільшення у валовому внутрішньому продукті (ВВП) частки інформаційних комунікацій та інформаційних продуктів і послуг, формування глобального інформаційного простору, здатного підтримувати ефективну інформаційну взаємодію людей і забезпечувати їм доступ до світових інформаційних ресурсів для задоволення їхніх соціальних та особистих потреб в згаданих вище продуктах і послугах [260].

Якщо говорити більш конкретно, то інформаційному суспільству притаманні такі ознаки:

– наявність єдиного інформаційного простору;

– домінування в економіці та управлінні нових технологічних укладів, що ґрунтуються на якнайширшому використанні інформаційно-комунікаційних технологій;

– підвищення значимості телекомунікаційної, транспортної та організаційної інфраструктури в системі суспільного виробництва і посилення тенденцій сумісного функціонування інформаційних і грошових потоків в економіці;

– збільшення важливості проблем забезпечення інформаційної безпеки особи, суспільства і держави, а також формування ефективної системи забезпечення прав осіб і соціальних інститутів на вільне розпорядження інформацією (отримання, розповсюдження, використання тощо);

– підвищення рівня освіти, що зумовлюється розширенням інформаційного міжнародного, національного та регіонального обміну, і як наслідок – підвищення значення кваліфікації, професіоналізму і творчих здібностей як найважливіших характеристик праці;

– перехід провідної ролі у забезпеченні сталого розвитку суспільства до інформаційних ресурсів;

– наявність у суспільства можливості задовольняти всі потреби в інформаційних продуктах і послугах.

Отже, найбільш поширеною є думка, за якою інформаційною безпекою слід вважати стан соціуму, за якого забезпечено надійний і всебічний захист особи, суспільства і держави від впливу на них особливого виду загроз, що мають вигляд певних інформаційних потоків, які були організовані або стихійно виникають і використовуються в інтересах регресивних, реакційних або екстремістськи налаштованих політичних і соціальних сил, спрямованих на свідому деформацію суспільної й індивідуальної свідомості, наслідком чого стають девіантна поведінка особи, посилення соціально-політичних, економічних і духовних колізій і через що зростає, розвивається й закріплюється психологічна і психічна напруженість соціуму [368].

На наш погляд, очевидним є те, що ефективна державна політика в інформаційній сфері, в тому числі в аспекті інформаційної безпеки, багато в чому залежатиме від правильного вибору пріоритетів у наукових дослідженнях цих проблем, розробки адекватних наукових моделей і підходів до їх вирішення [60]. Це, зокрема, стосується і потреби в державно-управлінському аналізі проблем інформаційної безпеки держав у сучасних умовах.

Тому доречно поділити думку відомого дослідника у сфері функціонування сучасної техногенної цивілізації С. Зубкова стосовно того, що рівень розробленості цього аспекту цієї проблематики є поки що невисоким [119, с. 15].

За наявних умов щоб досягти необхідного рівня інформаційної безпеки як невід’ємної частини нацбезпеки, треба чіткого знати й розуміти всі наявні та потенційні загрози, з якими зараз стикаються держави. Через це необхідно безперервно одержувати достовірну й повну інформацію не лише про загрози і ступінь їх небезпечності, а і про можливості впливати на них, щоб запобігти

їм, усунути їх, нейтралізувати або зменшити їх небезпечність. Такого стану можна досягти, обмежившись самими лише організацію та ефективним інформаційним забезпеченням нацбезпеки.

На нашу думку, інформаційне забезпечення нацбезпеки лише здається суто технічним питанням: воно охоплює специфічні філософські, економічні, державно-управлінські та соціокультурні моменти, бо такі речі, як наявність чи відсутність інформації, те, наскільки раціонально вона використовується і чи використовується взагалі, можуть мати величезні наслідки для особи, суспільства та держави, часом навіть руйнівні.

У зарубіжній і вітчизняній науці, а також у державно-управлінській практиці термін «національна безпека» почали активно використовувати на початку 90-х рр. XX ст. У першій чверті XXI ст. активізувалися дослідження, пов’язані безпосередньо із забезпеченням національної безпеки України. Більшість із них прямо чи опосередковано присвячено дослідженню категорії «національна безпека». Втім саме різноманіття визначень національної безпеки, які відрізняються одне від одного різними комбінаціями характеристик і навіть структурних компонентів [112], у цілому непогано відбивають усю її багатоаспектність, перш за все її сутнісний і функціональний аспекти.

Узагальнено національною безпекою вважається стан захищеності національних інтересів країни за наявності реальних і потенційних загроз [222, с. 40–43]. Національна безпека – стан, за якого в державі захищено національні інтереси країни в широкому їх розумінні, що включають політичні, соціальні, економічні, військові, екологічні, державно-управлінські аспекти, ризики, пов’язані із зовнішньоекономічною діяльністю, розповсюдженням зброї масового ураження, а також запобігання загрози духовним й інтелектуальним цінностям народу.

У цьому визначенні «безпека виступає як діяльність людей, суспільства, держави, світового співтовариства народів з виявлення (вивчення), попередження, послаблення, усунення (ліквідації) та відбиття

небезпек і загроз, здатних згубити їх, позбавити фундаментальних матеріальних і духовних цінностей, нанести неприйнятну (неприпустиму об'єктивно й суб'єктивно) шкоду, закрити шлях прогресивному розвитку» [216, с. 14–16], і в цьому сенсі скоріше йдеться не про саму безпеку, а про визначення її забезпечення.

Оскільки безпека, на нашу думку, – це передусім стан із певними параметрами і характеристиками, а реальну діяльність, насамперед органів державної влади, спрямовано на досягнення і підтримання цього стану, то можна йти висновку, що цей стан є не статичним, а динамічним.

Характер поняття «національна безпека» є конкретно-історичним, тобто у неї є пов'язані між собою минуле, сучасне і майбутнє, а розглядати цю безпеку необхідно неодмінно в просторі та часі. Зазначене важливо враховувати, організовуючи і здійснюючи її інформаційне забезпечення.

Отже, з урахуванням зазначених обставин, можна дійти висновку, що національна безпека є станом захищеності життєво важливих інтересів особи, суспільства та держави від зовнішніх і внутрішніх загроз і небезпек, який забезпечує надійне існування згаданих об'єктів, конкурентоспроможність і динамічний розвиток. Указане тлумачення терміна «національна безпека» надає можливість виділити два провідних напрямки її забезпечення: по-перше, захист від загроз і небезпек; по-друге, формування і підтримання умов для стабільного існування і динамічного розвитку. Перший напрям практично означає розбудову і функціонування системи протидії, здатної адекватно відповідати на згадані загрози й небезпеки, тоді як другий зосереджується на діяльності зі генерування і накопичення матеріального та духовного потенціалів і їх використання для реалізації національних інтересів. Із цього, на нашу думку, випливає положення про те, що в національній безпеці є щонайменше три аспекти:

– діяльнісний (нацбезпека як різноманітна діяльність суб'єктів з її забезпечення);

– ціннісний (вона ж як сукупність значимих для особи, держави і суспільства цінностей);

– персоніфіковано-індивідуальний (як результат діяльності, втіленої в людині).

Зазначене говорить про необхідність удосконалення інформаційних процесів і його важливість. Інакше кажучи, досягати безпеки завжди можливо лише за умов вивчення необхідної інформації (зокрема, про характер і ступінь конкретних загроз або небезпеки; про можливість їх уникнути, нейтралізувати або зменшити їх негативні наслідки; про реалізацію інтересів особи, суспільства і держави та її механізми тощо), де знайшли своє відображення елементи діяльності з досягнення її цілей.

Для інформаційного забезпечення дуже важливо виявити й визначити структуру нацбезпеки, що надає можливість з'ясувати види інформації, які циркулюють у розглядуваній сфері, і систему інформаційних зв'язків всередині неї та визначити суб'єкти й об'єкти нацбезпеки, що потребують певної інформації.

У науковій літературі існує кілька різних підходів до визначення елементів національної безпеки. Так, на думку відомого вченого В. Легасова, з огляду на характер джерел небезпеки, можна виділити сім таких елементів [167, с. 116–118]:

1) військово-політичний, що має на увазі виживання нації, недопущення за будь-яку ціну військової конфронтації;

2) промисловий – захист від стаціонарного або аварійного впливу потужних індустріальних об'єктів;

3) економічний – попередження подальшого неефективного господарювання країни;

4) політичний – недопущення гальмування процесів демократизації і гласності;

5) національно-культурний – збереження і захист історичних традицій і спадщини, попередження національних конфліктів; 6) гуманітарний – захист загальнолюдських цінностей;

7) соціально-політичний – захист соціальних досягнень радянського суспільства.

Інший дослідник – Б. Порфирьев – вважає, що нацбезпека містить у собі такі елементи:

– життя та здоров'я людей – екологічна безпека (охоплює і медичну);

– соціально-політичні права громадян і соціальних груп, умови їх життя, загалом політичний лад суспільства – соціально-політична або державна безпека;

– соціально-економічні права громадян, соціальних груп і всього суспільства та відповідні умови життя – соціально-економічна безпека;

– екологічні права громадян, соціальних груп і всього суспільства та відповідні умови життя – екологічна безпека;

– національно-культурні права громадян, соціальних груп і всього суспільства та відповідні умови життя – національно культурна безпека;

– військовий або оборонний потенціал цього суспільства або нації, державні (національні) кордони – військово-політична і державна безпека;

– економічний потенціал суспільства або нації загалом – економічна безпека [235, с. 11–12].

Ще одна досить поширена точка зору була сформульована російським вченим В. Мухіним, який розглядав усю сукупність загроз нацбезпеці і стверджував, що говорити про економічну, політичну, правову, воєнну, екологічну, інформаційну тощо загрози та відповідні види безпеки слід залежно від того, яким саме життєво важливим інтересам особи, держави та суспільства вони загрожують [211, с. 27].

Виходячи з вищевикладеного, ці види безпеки (економічна, політична, правова, воєнна, екологічна, інформаційна) є головними структурними складовими нацбезпеки [218].

Деякі автори вважають структурними елементами систему безпеки особи, систему безпеки держави та систему безпеки суспільства, розглядаючи їх як підсистеми системи нацбезпеки [216; 218; 227]. Видається, що останнє є правомірним, якщо йдеться про систему національної безпеки, а зазначені структурні елементи, хоча і є завершеними системами, проте виступають підсистемами системи більш високого порядку – системи зазначеної безпеки.

Цей підхід до дослідження структури нацбезпеки передбачає власний певний набір інформаційних зв'язків, які, як нам уявляється, багато в чому формують саму розглядувану систему безпеки. Усі основні типи зв'язків в їхній цілісності тут детально розглядати немає сенсу, достатньо підкреслити значущість саме згаданих інформаційних зв'язків системи забезпечення нацбезпеки. Такі зв'язки у розглядуваній сфері мають такий само складний і багаторівневий характер, як і структура цієї сфери. У найбільш загальному вигляді їх можна уявити як сукупність груп взаємозв'язків.

З одного боку, завдяки цим зв'язкам відбувається обмін інформацією між суб'єктами забезпечення нацбезпеки, завдяки чому підтримується організаційна цілісність системи.

З іншого боку, йдеться інформаційні зв'язки між людьми, діяльність яких безпосередньо чи опосередковано пов'язана із забезпеченням функціонування системи національної безпеки, а ще з одного – про інформаційні зв'язки між технічними компонентами цієї системи, адже в сучасних умовах певна частина інформаційних функцій, які окрема людина навіть не сприймає, але які є потрібними для забезпечення нацбезпеки, передається різним технічним засобам.

Загалом такі інформаційні зв'язки можна поділити на дві основні групи.

До першої з них належать змістовні інформаційні зв'язки, інформація в яких є структурною (пов'язаною). Зокрема, такими є зв'язки між елементами видів безпеки, між внутрішніми елементами кожного виду безпеки, між

конкретними видами безпеки та зовнішнім середовищем (під останнім тут розуміються національні інтереси інших країн) і т. ін.

До другої групи належать функціональні інформаційні зв'язки, що стосуються оперативної інформації. До таких можна віднести суб'єктно-об'єктні зв'язки (між суб'єктами, об'єктами, між суб'єктами й об'єктами, а також усередині них); зв'язки між суб'єктами, об'єктами та джерелами загроз, а також із зовнішнім середовищем.

Водночас усю сукупність інформаційних зв'язків, що стосуються нацбезпеки, можна поділити на зовнішні та внутрішні зв'язки.

Усі вони не існують поодинці, ізольовано один від одного, а перетинаються між собою та утворюють систему інформаційних відносин, яка є одним із найважливіших чинників, що визначають ефективність функціонування системи забезпечення нацбезпеки. Наголошуючи на важливості обміну інформацією для існування та розвитку будь-яких соціальних систем узагалі, Н. Вінер оголосив інформаційні зв'язки «цементом, що скріплює суспільство» [54, с. 31], а А. Берг і Б. Бірюков стверджували, що «якби живі істоти не мали органів чуття або інших "приладів" уловлювання інформації, або якщо б не існувало "інформаційного поля", життя на Землі не могло б ні виникнути, ні існувати» [28, с. 350].

Ясна річ, що і система забезпечення нацбезпеки не може ні виникнути, ні, тим паче, діяти як єдине ціле, якщо всередині неї не буде організовано процеси інформації. Необхідність такої організації обумовлюється багатьма чинниками, найважливішим із яких є необхідність вироблення цілей управління (у нашому випадку – управління державою) й отримання засобів їх досягнення, а також потребами самоорганізації системи [61].

Отже, без належної організації інформаційних зв'язків неможливо забезпечити цілеспрямовану поведінку системи в постійно мінливих умовах, неможливо пов'язати різноякісні компоненти в єдине, постійно діюче ціле й підтримувати систему в постійній готовності до виконання завдань, що виникають. А відсутність інформаційного обміну між компонентами системи

(у нашому випадку – системи держуправління) забезпечення нацбезпеки неминуче призведе до розладу між ними відносин функціонального типу, роз'єднання системи та її загибелі.

Отже, зазначена система інформаційних зв'язків дозволяє відшукати інформаційні потоки, з'ясувати їхні зміст і напрям, і це, в свою чергу, надає можливість раціонально використовувати інформаційні ресурси та потенціал, щоб забезпечити суб'єктів нацбезпеки найбільш повною, достовірною та своєчасною інформацією [315].

Наявність такої складної, динамічної структури національної безпеки, а також системи інформаційних зв'язків, розглянутих вище, зумовлює й наявність великої кількості інформаційних потоків.

Звісно ж, що їх можна класифікувати за тим само принципом, що й інформаційні зв'язки. Зупинимось трошки на характеристиці найважливіших із них. До таких, на нашу думку, належить поділ на внутрішні та зовнішні; на висхідні, низхідні й горизонтальні, а також на прямі та зворотні.

Під зовнішнім потоком інформації мається на увазі її рух від глобальної (загальносвітової), регіональних та різних національних систем безпеки до конкретної системи нацбезпеки. Він зв'язує останню із системою зовнішніх небезпек та загроз і водночас із системами безпеки такого ж само та більш високого порядку. На відміну від зовнішнього, внутрішній потік поєднує в єдине ціле структури, що забезпечують національну безпеку, між собою та із суб'єктами й системою внутрішніх небезпек і загроз. У цьому разі інформація відображає всі боки державно-управлінської, економічної, правової та іншої діяльності суб'єктів нацбезпеки із реалізації життєво важливих інтересів і забезпечення стабільності особи, суспільства та держави.

Інформація, що міститься у внутрішньому й зовнішньому потоках, може бути найрізноманітнішою за змістом і формою. Наприклад, за змістом вона може виявитись державно-управлінською, правовою, воєнною,

соціальною тощо, а за формою – задокументованою, зафіксованою в електронному вигляді, усною тощо).

Висхідним потоком вважається рух інформації знизу вгору, який формують окремі особи, керівники низових ланок державної влади та самоуправління, політичних і громадських організацій та інших низових структур і в якому відображаються результати діяльності з реалізації та захисту життєво важливих інтересів окремих осіб, колективів і соціальних груп. Він може сягнути верхніх рівнів політичної та державної влади як найважливішого елемента системи забезпечення нацбезпеки. Низхідний потік, навпаки, є рухом інформації від верхніх рівнів розглядуваної системи до її підґрунтя чи то від вищих щаблів політичної та державної влади до окремих осіб, їх груп чи колективів.

Особливістю горизонтального потоку є його циркулювання на одному ієрархічному рівні відповідної системи (у нашому випадку – системи нацбезпеки). Він виступає потоком взаємодії.

Для сфери держуправління системою забезпечення нацбезпеки найбільш характерними є прямі та зворотні інформаційні потоки, саме завдяки їх існуванню система зберігає динамічну рівновагу. Прямими (від суб’єкта управління до об’єкта) та зворотними (від об’єкта управління до суб’єкта) потоками передаються величезні масиви відомостей про функціонування системи забезпечення нацбезпеки. Отримана завдяки ним інформація надає можливість коригувати як правильність ухвалення рішень, насамперед на вищих щаблях управління, так і діяльність з їх втілення в життя [176].

Отже, у сфері нацбезпеки невпинно рухаються найрізноманітніші інформаційні потоки, які можуть тісно переплітатися чи накладатися один на одного і подекуди дублювати інформацію, яку вони передають. Тому для вдосконалення інформаційного забезпечення нацбезпеки дослідження та оптимізація цих потоків має бути пріоритетним напрямком.

Якщо ж повернутись до питання інформаційної функції системи нацбезпеки, то її змістом є отримання системою в цілому та її елементами інформації, потрібної для здійснення узгодженої і цілеспрямованої діяльності з досягнення цілей цієї безпеки.

Вимоги до цієї функції диктують потрібність і достатність інформації, що надається споживачеві відповідно до його запитів, тобто інформаційні потреби та можливості їх задовольняти. При цьому питання про інформаційні потреби споживачів інформації не лише у сфері нацбезпеки, а і в будь-який інший, вважається досить дискусійним і проблематичним.

Ми виходимо з того, що зазначені потреби є похідними від функцій споживачів і їх ролі у забезпеченні нацбезпеки, а тому формуються на основі моделювання процесу її забезпечення. Це пояснюється тим, що значну кількість небезпек і загроз (такі, як інформаційна війна, економічна криза, природні катаклізми тощо) ми маємо можливість лише змоделювати і, відповідно, так само змоделювати діяльність з їх нейтралізації або усунення.

1.2. Інформаційне забезпечення державної політики як важливий чинник безпеки держави

Інформаційне забезпечення – це особливий вид забезпечення, зумовлений специфікою самого продукту забезпечення – інформацією. Інформаційні ресурси в останні десятиліття набувають все більшого значення у функціонуванні сучасних держав. Тому не випадково ще на зорі свого існування у розвитку людської цивілізації виділялося два напрямки діяльності: матеріальне виробництво та інтенсифікація інформаційних процесів.

У сучасному житті людини й людського суспільства інформація відіграє найважливішу роль. Спілкування, пізнання, знання минулого і прогноз на майбутнє, існування держави, виробництво матеріальних благ, їх

розподіл і споживання та багато іншого можливі тільки й завдяки отриманню, переробці, зберіганню і використанню інформації.

На наш погляд, інформація у XXI ст. стає такою ж загальною категорією, як матерія або енергія. Вона дедалі частіше виступає основним ресурсом влади поряд із силовою та фінансовою складовими; пронизує всі сфери життєдіяльності особи, суспільства та держави, є безпосереднім державно-управлінським ресурсом і поряд із сировиною та енергією – одним з основних багатств країни, її національним надбанням.

Без своєчасної й достовірної інформації є практично неможливим функціонування жодного виду забезпечення нацбезпеки, серед іншого і державної безпеки, яка виступає як підсистема національної. Саме інформація є тим компонентом, який притаманний будь-якому з видів забезпечення національної безпеки. Цим і зумовлюються специфіка й особлива роль інформаційного забезпечення.

В усіх найрозвиненіших державах інформаційному забезпеченню нацбезпеки надається дуже важливе значення. Так, у документі «Стратегії національної безпеки США» зазначається: «Наша стратегія національної безпеки формулюється виходячи з американських інтересів і цінностей. Прихильність США свободі, рівності та людській гідності продовжує залишатися маяком надії для народів усього світу. Життєздатність, творча енергія та різнобічність американського суспільства є важливим джерелом національної могутності в системі глобальної економіки, рушійними силами якої все більше стають нові ідеї та інформаційне забезпечення [264, с. 8].

Теоретичну основу досліджень у сфері інформаційного забезпечення державної влади становлять роботи зарубіжних авторів Д. Белла, Е. Тофлера, М. Кастельса і М. Маклюена, вітчизняних дослідників О. Бухтатого, С. Луценко, О. Крюкова, Г. Почепцова, В. Степанова, С. Чукут та ін.

Завдання цього підрозділу полягає у вивченні інформаційного забезпечення як особливого виду управління, в основі якого лежить роль

інформації у діяльності органів державної влади, та її впливу на проблеми безпеки держави.

Для забезпечення нацбезпеки необхідно здійснювати цілий комплекс різних видів діяльності: політико-дипломатичної, державно-управлінської, економічної, правової, військової, інформаційної, що спрямовані на досягнення й підтримання необхідного її стану.

Ефективність такої діяльності значною мірою визначається наявністю стійких інформаційних зв'язків, кількістю інформаційних потоків, їх характером, змістом і якістю, тобто інформаційним забезпеченням нацбезпеки.

Особливістю і відмінною, специфічною рисою інформаційного забезпечення від решти різновидів забезпечення нацбезпеки є сам особливий продукт її забезпечення – інформація, оскільки вона лежить у підґрунті будь-якої діяльності людини і через це слугує необхідною умовою її раціонального життєзабезпечення.

Отже, національна безпека є складною, динамічною, цілісною соціальною системою, компонентами якої є підсистеми безпеки: держави, особи та суспільства. Саме взаємопов'язана, системна єдність останніх становить якісну визначеність, покликану захисти життєво важливі інтереси держави, особи та суспільства, забезпечити їх конкурентоспроможний, прогресивний розвиток.

Ключовим елементом, завдяки якому може існувати цілеспрямована координація зусиль усіх державних і громадських сил щодо забезпечення нацбезпеки, є система відповідного державного управління. У свою чергу, для здійснення цілеспрямованих та ефективних управляючих впливів (у нашому випадку їх метою є забезпечення нацбезпеки, але це стосується і всіх інших життєвих сфер) потрібна достовірна, об'єктивна, повна та своєчасна інформація. Отримати її суб'єкти нацбезпеки можуть завдяки наявності інформаційного забезпечення розглядуваної сфери.

У XXI ст., для якого є характерним інтенсивне проникнення сучасних інформаційних технологій у всі сфери життєдіяльності суспільства, залежність національної безпеки від наявності потрібної і достатньої для її забезпечення інформації стрімко зростає. Швидкий розвиток інформаційних технологій обіцяє невдовзі призвести до того, що левова частка інформаційного ресурсу держави набуде електронної форми. Ця досить реальна перспектива примушує шукати нові ефективні та раціональні шляхи отримання, обробки й використання інформації та її кращого захисту і зберігання. Останнє стає дедалі важливішим, бо значно підвищується залежність від збереження інформації (до речі, як і від її повноти) стабільності у суспільстві, забезпечення прав і свобод громадян, правопорядку і навіть такі масштабні питання, як збереження цінностей держави, більш того – самої її цілісності, збереження традицій і звичаїв нації та підвалин її самоідентифікації.

Інакше кажучи, потреба окремих осіб і соціальних груп, суспільства та держави в інформації, тобто в надійному, ефективному та своєчасному інформаційному забезпеченні, наразі є об’єктивною. Не буде перебільшенням вважати, що інформаційне забезпечення нині виступає не лише невід’ємною частиною системи нацбезпеки, а й однією найголовніших умов її існування.

У науковій літературі існують різні визначення інформаційного забезпечення. Так, за однією із точок зору «інформаційне забезпечення – це сфера професійної науково-інформаційної діяльності для задоволення суспільних, колективних та індивідуальних потреб» [37, с. 120].

Деякі науковці вважають, що «інформаційне забезпечення являє собою організований безперервний технологічний процес підготовки та видачі інформації споживачам відповідно до їх потреб для підтримки ефективної науково-технічну діяльність» [125, с. 222–224], тоді як інші стверджують, що «інформаційне забезпечення – це перш за все специфічна діяльність,

спрямована на реалізацію комплексного процесу з підготовки та доведення інформації до фахівців» [265, с. 111, 113, 115].

Більш розширене трактування цього поняття виглядає так: «Під інформаційним забезпеченням науково-дослідних і дослідно-конструкторських робіт розуміється комплексний, цілеспрямований процес доведення інформаційних матеріалів, створених у сфері документального, фактографічного і концептуального обслуговування, до безпосередніх виконавців розробки з урахуванням їх інформаційних потреб і наявних інформаційних ресурсів (методів, засобів тощо)» [175, с. 41–45].

Процитовані визначення інформаційного забезпечення відповідають практиці, тож, усі можуть вважатись слушними. Їх відрізняє головним чином повнота характеристик, натомість деякою мірою вони доповнюють одне одного. Як випливає із зазначених визначень, спільним для них є згадка про те, що інформаційна діяльність виражається в інформаційному процесі, а також про наявність споживачів інформації та їхні інформаційні потреби, комплексність і цілеспрямованість, відсилка до якої обумовлюється тим, що, з одного боку, для вирішення будь-яких завдань доводиться використовувати різні види інформації, а з іншого – остання потрібна для здійснення певної діяльності, яка неодмінно має якусь мету [312].

У найзагальнішому розумінні інформаційне забезпечення – це завжди специфічна діяльність, спрямована на підготовку і доведення інформації до відома її споживачів. Збирання, обробка, зберігання та передання інформації є інформаційним процесом, притаманним будь-якій сфері чи галузі життєдіяльності людини під час здійснення інформаційного забезпечення. Втім, для визначення більш конкретного інформаційного забезпечення – такого забезпечення нацбезпеки – необхідно визначити саме його специфічні риси, визначені особливостями розглядуваної сфери.

Головна особливість інформаційного забезпечення взагалі і загалом полягає в тому, що під час нього нова інформація не створюється, а збирається вже існуюча, потім обробляється і надається споживачеві у

зручній для нього формі. У свою чергу, процес підготовки інформації спрямовано на створення інформаційних ресурсів, під якими у розглядуваній сфері в найвужчому сенсі мається на увазі сукупність документів, їх масивів та баз даних, що містяться в інформаційних системах (архівах, банках даних, фондах тощо). Саме завдяки існуванню таких інформаційних ресурсів споживач має можливість одержувати потрібну йому інформацію, через це створення таких ресурсів у сфері нацбезпеки перетворюється на завдання загальнонаціонального масштабу, оскільки від них значною мірою залежить ефективність інформаційного забезпечення відповідних споживачів інформації [188—191].

Іншою суттєвою особливістю інформаційного забезпечення державної нацбезпеки є те, що воно здійснюється в суворій відповідності до інформаційних потреб суб'єктів такої безпеки. Лише в цьому разі реально створити умови для ефективної діяльності відповідних інформаційних структур і їх працівників щодо забезпечення інформацією тих, хто її потребує.

Крім цього, призначенням інформаційного забезпечення є сприяння інформаційними засобами підвищенню ефективності загальної діяльності системи забезпечення державної та національної безпеки, тобто допомога безпосередньо в досягненні цілей нацбезпеки.

Як у же наголошувалося раніше, за характером інформаційне забезпечення нацбезпеки є цілеспрямованим, і мета у цьому разі слугує його важливим системоутворюючим чинником.

Повертаючись до визначення, можемо сформулювати його таким чином: інформаційне забезпечення національної безпеки – цілеспрямований, специфічний і безперервний процес збирання, аналізу, збереження та надання суб'єктам нацбезпеки інформації, потрібної для її забезпечення, який здійснюється спеціально створеними для цього органами, інститутами або службами суспільства і держави.

Головні риси, зафіксовані в цьому визначенні, відображають сутність інформаційного забезпечення нацбезпеки. У цілому його сенс можна звести до того, щоб суб'єкти забезпечення нацбезпеки можуть завдяки йому своєчасно отримували у необхідній і достатній кількості та зручній формі потрібну їм достовірну й повну інформацію про національних інтересів і загрози цим інтересам. Втім, на наш погляд, система нацбезпеки належить до складних соціальних систем, що складаються з великої кількості різних за функціями і змістом елементів, які зумовлюють її структуру.

Вважаємо, що одним із системоутворюючих чинників цієї системи є інформація, точніш – інформаційні зв'язки, що складаються у процесі її взаємодії із зовнішнім середовищем та її складовими елементами. Унаслідок цієї взаємодії поряд з іншими обмінами відбувається і інформаційний обмін, завдяки якому може з'являтися нова інформація. Тому інформаційне забезпечення нацбезпеки можна розуміти і в більш широкому сенсі, а саме як інформаційну взаємодію розглядуваної системи із зовнішнім середовищем і між її складовими елементами. Саме таке розуміння інформаційного забезпечення нацбезпеки надає можливість визнавати її структурними елементами також і ті державні органи та служби разом з організаціями громадянського суспільства, які спеціально з таким призначенням не створювалися, однак з різних причин виконують функції збирання та надання інформації, потрібної для досягнення цілей нацбезпеки.

Також запропоноване розширене тлумачення інформаційного забезпечення нацбезпеки надає можливість коректно використати поняття «інформаційне середовище» (таким вважаються сфери діяльності суб'єктів, пов'язані зі створенням, перетворенням і споживанням інформації), що виступає, з одного боку, провідником, перетворювачем і розповсюджувачем інформації, а з іншого – джерелом спонукань людської діяльності.

Оскільки інформаційне забезпечення національної безпеки є самостійним процесом, у нього є власні цілі та завдання. З огляду на це інформаційне забезпечення як умову надійного функціонування системи

забезпечення безпеки можна описати і як процес збирання (отримання) та надання інформації і налагодження комунікацій, які уможливлюють вільну циркуляцію інформації, її вільне, але збалансоване поширення, гарантують різноманіття джерел інформації, вільний доступ до них і забезпечення прав людини у розглядуваній сфері.

Мети такого забезпечення можна досягти шляхом вирішення конкретних завдань у розглядуваній сфері, а саме:

– забезпечення найповнішого та своєчасного надання інформації її споживачам у сфері нацбезпеки;

– масштабна інформаційна взаємодію щодо виявлення джерел небезпеки та загроз на різних рівнях безпеки;

– поліпшення поширення, полегшення доступу та обміну інформацією щодо джерел небезпеки і загроз на всіх рівнях;

– удосконалення процесів розповсюдження, доступу та обміну інформацією з питань співпраці у забезпеченні національної, колективної і глобальної безпеки;

– формування громадської думки стосовно проблем забезпечення нацбезпеки як на міжнародному рівні, так і всередині держави;

– поліпшення стилю роботи інформаційних структур і фахівців.

Цілі та завдання визначають специфіку змісту інформаційного забезпечення нацбезпеки й вимоги, які до неї. Висуваються. Її специфіка, у свою чергу, знаходить свій прояв у функціях, тобто в тій ролі, яку отримує процес надання інформації на різних етапах забезпечення нацбезпеки.

Варто підкреслити, що функціональний аналіз як складова частина системного аналізу знайшов широке застосування у дослідженнях соціально-політичних явищ і процесів.

По-перше, функції інформаційного забезпечення відображають ті ролі, які воно виконує відносно національної безпеки як системи та її окремих компонентів. При цьому важливо відзначити, що функції властиві як системі інформаційного забезпечення, так і окремим його компонентам.

По-друге, функція розглядається як форма, спосіб прояву активності системи та її компонентів. Тут мається на увазі, що інформаційне забезпечення, об'єктом якого виступає національна безпека, є не лише своєрідним відображенням практики забезпечення нацбезпеки, а і те, що його головним призначенням є активний вплив на процес забезпечення безпеки особи, суспільства та держави.

По-третє, оцінюючи призначення і практичне значення інформаційного забезпечення у сфері нацбезпеки, необхідно розуміти і пізнавальну проблему. інформаційне забезпечення за своєю природою є динамічним явищем, однак у наукових цілях під час дослідження його функціональної ролі у розглядуваній сфері його доводиться застосовувати до статичного стану цього явища, тобто в певних випадках доводиться тимчасово абстрагуватися від динаміки зміни інформаційного забезпечення.

По-четверте, далеко функції інформаційного забезпечення нацбезпеки в різних державах з різними політичними режимами мають зовсім неоднакові прояви. Так, у державах з демократичним ладом зазвичай є всі необхідні умови для найповнішої реалізації функцій інформаційного забезпечення в усіх сферах, серед іншого і в безпековій, і зовсім інша річ – здійснення інформаційного забезпечення в умовах повного або часткового обмеження державою циркуляції інформації. Через це пропонуємо краще зупинитися на загальних моментах функціонування, не вдаючись у детальний аналіз інформаційного забезпечення цієї безпеки за різних політичних режимів.

Слід наголосити, що в українській науковій літературі функціям, які виконуються інформаційним забезпеченням нацбезпеки, наразі приділено недостатньо уваги, що зумовлює необхідність їх виокремлення й більш детального розгляду. Зокрема, до згаданих функції можна віднести такі:

– соціалізації інтересів і пріоритетів нацбезпеки;

– раціоналізації процесу забезпечення цієї безпеки;

– деідеологізації (за партійною ознакою) суб'єктів забезпечення нацбезпеки;

– формування ціннісної орієнтації суб’єктів та об’єктів нацбезпеки;

– налагодження взаємодії системи цієї безпеки із системами регіональної та міжнародної безпеки;

– забезпечення прогнозування її стану.

Перш за все варто зауважити, що формування національних інтересів, їх осмислення та реалізація є складним і комплексним процесом, який здійснюється у правовій державі на демократичній основі. У ньому беруть участь практично всі інститути та органи, з яких утворюється політична організація суспільства, а саме:

– інститути держави (органи законодавчої, виконавчої та судової гілок влади);

– недержавні інституції (політичні партії та рухи, громадські об’єднання та організації);

– ЗМІ, що представляють інтереси найрізноманітніших верств населення, соціальних груп, державних і громадських структур.

Ця сукупність інтересів містить у собі життєво важливі інтереси окремої особи, держави та суспільства, які в сукупності, разом узяті і стаються національними інтересами. При цьому презентуються не самі інтереси, а відомості про них.

Річ у тому, що появу національних інтересів можна уявити собі як процес передання інформації від окремої особи до соціальної групи, суспільства та держави, а потім з усієї сукупності інформації про їхні інтереси добираються дані, які свідчать про життєво важливі інтереси об’єктів національної безпеки, а саме особи, суспільства та держави. Це надає можливість говорити вже про функції соціалізації інформаційного забезпечення нацбезпеки.

І справді, для здійснення функція соціалізації інтересів і пріоритетів національної безпеки необхідно спочатку виявити інформацію для визначення самих національних інтересів, а також отримати інформацію, потрібну для вибору з можливих альтернатив і схвалення найбільш

прийнятної моделі забезпечення нацбезпеки. Тут варто зауважити, що національні інтереси є величиною постійною лише в певний період часу, вони постійно змінюються, що зумовлює необхідність постійно мати інформацію про життєво важливі інтереси. Цей процес відбувається за допомогою інформаційної артикуляції та агрегації інтересів.

Перше передбачає постійне надання інформації про інтереси об'єктів безпеки особам, які ухвалюють рішення у сфері нацбезпеки, а друге – перетворення самих інтересів на національні інтереси.

Крім того, національна безпека забезпечується вибором певних моделей діяльності, при цьому ця модель може не завжди знаходити підтримку в об'єктів безпеки. Через це суб'єкти нацбезпеки змушені чинити інформаційний вплив на них з метою обґрунтування вибору саме цього шляху її забезпечення.

Прикладом може послужити діяльність адміністрації США під час підготовки до проведення операції «Буря в пустелі». Шляхом цілеспрямованого подання інформації своїм громадянам американській владі вдалося сформувати громадську думку щодо необхідності проведення цієї операції й отримати підтримку громадян.

Функція раціоналізації процесу забезпечення нацбезпеки передбачає надання такої інформації, яка дозволить забезпечити вибір оптимального шляху досягнення цілей безпеки. Це обумовлює наявність необхідної й достатньої інформації для ухвалення оптимального рішення та ефективного використання сил і засобів забезпечення цієї безпеки.

Інакше кажучи, функція раціоналізації здійснюється шляхом інформаційного супроводу процесу вирішення завдань нацбезпеки, тобто постійного надання інформації про стан, структуру і динаміку загроз, результати впливу на них, ставлення народу до урядової політики у безпековій сфері, ступінь реалізації життєво важливих інтересів особи, суспільства та держави, їх задоволеність ступенем безпеки, соціальні оцінки і прогнози тощо. Інакше кажучи, роль інформаційного забезпечення у сфері

нацбезпеки є унікальною, бо воно є пов’язаним із мудрістю і досвідом народу, містить багатющу гаму суджень щодо проблем цієї безпеки, а головне – надає можливість вибирати найкращі шляхи та найефективніші способи вирішення цих проблем.

Ця функція охоплює всі види планування та прогнозування діяльності інформаційних систем, їх координацію, встановлення прямих і зворотних зв’язків, а також організацію інформації в аксіологічному, семантичному, семіотичному та інших аспектах.

Маючи необхідну інформацію, керівництво країни виробляє найбільш оптимальний варіант забезпечення національної безпеки й раціонально використовує для цього наявні сили і засоби.

Тож, інформаційне забезпечення нацбезпеки постачає владні структури найбільш цінною інформацією. Цінність же останньої нерідко визначається ефективністю діяльності інформаційних структур, які здійснюють свою діяльність у розглядуваній сфері.

Функція деідеологізації (за партійною ознакою) суб’єктів цієї безпеки забезпечує, перш за все, доступність джерел інформації і відкритість самої інформації для її споживачів у розглядуваній сфері. Вона є важливою, оскільки забезпечення всеосяжною, достатньо об’єктивною інформацією суб’єктів та об’єктів нацбезпеки є найважливішим важелем взаємного контролю й перешкодою на шляху насадження партійних (корпоративних) інтересів, які можуть подаватися як інтереси національні. Виконання цієї функції є важливою складовою частиною демократичних механізмів взаємодії держави і громадянського суспільства й виступає важливою умовою реалізації та захисту національних інтересів, оскілки передбачає досить вільну циркуляцію інформаційних потоків у країні.

Аналізуючи ці функції, варто зауважити, що їх розмежування в теорії є досить умовним. Насправді вони тісно переплітаються одна з одною, є взаємно пов’язаними, можуть накладатися, перекриватися, частково доповнювати й заміщувати одна одну.

Нарешті, прояв цих функцій значною мірою визначається ступенем зрілості громадянського суспільства та інших значущих демократичних інститутів.

Розбудови, організації, раціонального функціонування та ефективного використання інформаційного забезпечення національної безпеки можна досягти, якщо дотримуватися певних принципів. Видається, що найбільш важливими з них є такі.

1. Повнота інформаційного забезпечення, сенс якої полягає в тому, що пошуку повинен видавати інформацію в повному обсязі, зводячи водночас до мінімуму «шум» і виключаючи дезінформацію. Головне для цього – вибрати таку пошукову стратегію, щоб споживач мав можливість одержувати інформацію, яка відповідатиме не лише запитаній тематиці, а і його інформаційним потребам.

2. Актуальність інформаційного забезпечення, завданням якого є вчасне надання споживачеві пріоритетної інформації, що відповідає його запиту.

3. Точність і надійність інформаційного забезпечення, під чим мається на увазі надання споживачеві всієї потрібної інформації, що матиме бажані вид і мовне оформлення, заданої хронологічної глибини тощо.

4. Інформація повинна подаватись у зручній для споживача формі (машинопис, мікрофільм, екран дисплея тощо).

5. Диференційованість інформаційного забезпечення, що передбачає врахуванням завдань споживача, його статусу та оперативності завдань, які він має виконувати.

6. Системність інформаційного забезпечення, що полягає в систематичному задоволенні інформаційних потреб на всіх етапах забезпечення нацбезпеки і комплексності видів інформаційного забезпечення з урахуванням категорій споживачів, характеру їх інформаційних запитів та специфіки завдань, які вони вирішують.

Реалізація цих принципів може бути більш ефективною з урахуванням низки обставин, які безпосередньо впливають на них, а саме:

а) постійне вивчення закономірностей, проблем і завдань забезпечення як нацбезпеки загалом, так і її окремих напрямків, що дозволить виявити групи споживачів інформації, сформулювати їх інформаційні потреби і запити, а також виділити джерела інформації про небезпеки і загрози;

б) створення і введення нової системи довідково-інформаційних фондів, що дозволить здійснювати швидкий пошук і подання інформації, що стосується нацбезпеки;

в) активне використання сучасних інформаційних технологій та автоматизованих інформаційних систем, що дозволяють здійснити інтенсифікацію інформаційних процесів і потоків у цій сфері;

г) планування інформаційної діяльності в цілому і окремих її напрямків, що забезпечить взаємодію як між видами інформаційного забезпечення, так і із зовнішнім середовищем.

Для практичної реалізації інформаційного забезпечення нацбезпеки потрібна розбудова адекватної інформаційної системи, яка здійснюватиме діяльність з доставки суб’єктам нацбезпеки потрібної інформації. Для цього необхідно вирішити методологічно важливе питання про сутність інформаційної системи. У науці це питання наразі досліджено вже досить широко [326]. Практично всі дослідження так чи інакше ґрунтуються на узагальненій моделі інформаційної системи, запропонованої К. Шенноном, який виділяв такі її основні елементи:

1) джерело інформації;

2) передавач інформації;

3) канал її передання;

4) приймач;

5) адресат або споживач інформації.

Оскільки національна безпека – явище соціальне, найбільш доречно застосовувати для нього терміни «спілкування» або «комунікація».

«Комунікація» (лат. «Communication» від «communico» – роблю спільним, пов’язую, спілкуюся) – це насамперед спілкування або передання інформації від людини до людини в процесі діяльності, завдяки чому передавач, канал і приймач є сенс прирівняти до комунікації або комунікаційного каналу [355].

Слід підкреслити, що така модель має спрощений характер, однак є досить зручною для розуміння суті процесу подання інформації.

Для формування інформаційної системи у сфері нацбезпеки треба спочатку визначити специфічний зміст зазначених вище компонентів.

Говорячи про джерело інформації, перш за все, варто поділити думку М. Янкова, що «джерело інформації і інформація – це дві різні речі. Їх не слід ототожнювати».

Двоїстість природи інформації заважає шукати її однаково як у джерелі, так і в її одержувача. На погляд М. Янкова, «дійсне джерело інформації – це система, властивості якої відображаються в одержуваній, перетворюваній і використовуваній інформації» [332].

У філософсько-методологічній класифікації знайшли відображення всі наявні джерела інформації, а її головний об’єктивний критерій ґрунтується на врахуванні найзагальніших інформаційних інтересів суб’єктів нацбезпеки. За такого підходу джерела інформації можна групувати за рушійними силами (природні та соціальні), за сферами прояву (політичні, економічні, технічні, військові і т. ін.);, за масштабними ознаками та за способами і формами дії.

Зміст кожного елемента критерію є складним. Зокрема, деякі основні ознаки класифікації джерел інформації відображали такі їх властивості, як просторовий масштаб (глобальні, регіональні, локальні, місцеві), тривалість дії (короткочасні, середньострокові, довгострокові), термін служби (постійні, мінливі), доступність широким масам (доступні, з обмеженим доступом, закриті) тощо

Ключове, найголовніше значення має критерій класифікації джерел інформації відповідно до потреб суб’єктів нацбезпеки. Річ у тому, що потреби суб’єктів – це те, що становить їх суть і їх задоволення забезпечує

саме існування суб'єктів, є головною причиною їх діяльності. А для здійснення діяльності завжди необхідна відповідна інформація. Наявність інформації є умовою діяльності, у цьому випадку з реалізації національних інтересів та їх захисту. Справді, перш ніж що-небудь робити, ми збираємо потрібні відомості, аналізуємо їх, потім, лише прийнявши рішення, починаємо діяльність. Слід зауважити, що інформація завжди має цілком певне джерело.

Разом із тим, якщо позбавити суб'єктів можливості отримувати інформацію, необхідну для забезпечення національної безпеки, це призведе до їх загибелі, деградації, втрати власних ознак. Тож, природньо, що для захисту власних інтересів люди насамперед прагнуть отримати найбільш повну і водночас об'єктивну й достовірну інформацію, що б на її підставі найбільш ефективно обстоювати власні інтереси.

Отже, з'ясувавши інтереси суб'єктів нацбезпеки, не важко встановити, якої саме інформації вони потребують, або інформація про які процеси та явища є для них найважливішою у цей момент часу. Більш того, через те, що інтереси одних можуть не лише відрізнятися від інтересів інших, а і входити з ними у суперечність чи антагоністичний конфлікт, та ж сама інформація для одних може бути життєво необхідною, а для інших – надлишковою або просто непотрібною. Тому є всі підстави вважати, що саме інтереси суб'єктів нацбезпеки мають слугувати найважливішим критерієм класифікації джерел інформації відповідно до таких їх особливостей, як спрямованість, адресність, пріоритетність, доступність та ін.

Іншим висновком із цього є те, що для класифікації джерел інформації, треба розуміти і класифікацію самих цих інтересів. З огляду на зазначене варто зупинитись на класифікації інтересів, відповідно до якої вони розрізняються за: 1) ступенем спільності (особисті, групові, національні, глобальні); 2) характером суб'єкта (інтереси особи, держави, суспільства); 3) сферою прояву (політичні, економічні, соціальні, військові тощо) та інші [313]. За тією ж логікою серед джерел інформації можна вирізняти

індивідуальні, групові та масові; за доступністю – відкриті, спеціальні та закриті, а джерелами такої інформації можуть виступати окремі особи, різноманітні соціальні групи, суспільство в цілому, держава та її інститути.

На завершення підтеми класифікації інформації за критерієм інтересів суб'єктів нацбезпеки, варто побудувати відповідну ієрархічну схему, розташувавши їх за значущістю. У підґрунтя цієї ієрархії можна покласти підхід, запропонований авторським колективом під проводом В. Серебряннікова, за яким національні інтереси охарактеризовано як: «а) найбільш істотні інтереси (життєво важливі); б) суттєві (ключові); в) малоістотні (третьорядні); г) несуттєві» [257]. Аналогічно можна поділити за значимістю джерела інформації: а) життєво важливі (дозволяють одержувати інформацію про всі найбільш небезпечні загрози); б) суттєві (надають можливість одержувати інформацію взагалі про всі небезпеки); в) малосуттєві (надають можливість одержувати інформацію про можливі небезпеки), г) несуттєві (дозволяють одержувати інформацію про можливі передумови до появи небезпек). Зауважимо, що значимість зазначених джерел може змінюватися, якщо змінюється ситуація, тому така класифікація лишається дієвою тільки на конкретний момент часу.

Нині головним джерелом інформації для розвитку особи чи соціальної групи слугують ЗМІ, насамперед телебачення та радіо, завдяки яким люди отримують головний масив відомостей про стан нацбезпеки, небезпеки, що їй загрожують та про те, як їх можна нейтралізувати, тоді як для політичного керівництва країни на першому місці серед джерел інформації перебувають інститути, органи і служби, створені саме із цією метою, завданнями та функціями яких є безпосереднє одержання і передання відомостей, потрібних для забезпечення нацбезпеки. До таких належать, зокрема, органи розвідки і контррозвідки, серед іншого радіоелектронної, інформаційні структури військового відомства, Міністерство внутрішніх справ Міністерство закордонних справ і ціла низка інших органів, служб та інституцій.

Щодо видів і типів інформації варто згадати, що інформація в системі нацбезпеки, яка є складним, багатоплановим соціально-політичним явище, може циркулювати вкрай різноманітна, тож, і класифікувати її можна за дуже різними підставами. Зокрема, за походженням відносно об'єктів національної безпеки вона може поділятись на вхідну і вихідну або на зовнішню і внутрішню, а за значенням для цих об'єктів можна розрізнити повідомлення, коментар, аналітичну і синтезовану інформацію.

За роллю, виконуваною інформацією в системі нацбезпеки, її можна поділити на оперативну й структурну (пов'язану), корисну, нейтральну та шкідливу. Мабуть, доцільно розрізняти також такі її різновиди (чи то аспекти), як гносеологічний, прагматичний, аксіологічний, семантичний та інші, тоді як відштовхуючись від функції інформації в процесі забезпечення цієї безпеки можна виділити директивну, організаційну, нормативну, довідкову, контрольну інформацію тощо. Якщо ж узяти критерієм тип носія інформації, то стає доречно поділити її усну та друковану, зорову і слухову, документовану, радіоелектромагнітну тощо.

При цьому через те що для забезпечення національної безпеки необхідно зберігати певну діяльність більшою чи меншою мірою в таємниці, є сенс згадати і про такий критерій класифікації як відкритість, або ступінь доступності такої інформації. Таким чином, інформацію можна поділити на відкриту (призначену для масового споживання), спеціальну (яка використовується вже не для масового споживання, але ще не вважається державною таємницю) та закриту (визнану державною таємницею).

Крім того, класифікувати інформацію можна за такими підставами, як її новизна, актуальність, зміст, положення конкретного джерела в ієрархічній системі органів управління національної безпеки тощо. Водночас відповідно до характеру загроз і небезпек для тих чи інших сфер життєдіяльності особи, суспільства та держави її можна поділити на політичну, економічну, соціальну, правову, воєнну, демографічну, техніко-технологічну, екологічну та ін. – цей перелік можна продовжити відповідно до видів безпеки.

Від джерела інформація передається до споживача різними каналами. Із них для інформаційне забезпечення нацбезпеки використовуються насамперед такі два:

1) офіційний (цим каналом циркулює інформація з високим ступенем вірогідності, форму, зміст і час подання якої чітко регламентовано);

– неофіційний (ним некеровано надходить величезна кількість різних відомостей, що далеко не завжди об'єктивно характеризують справжній стан справ).

У принципі, ці канали функціонують завжди, але важливо, щоб забезпечення споживачів об'єктивною, повною, регламентованою за формою і часом подання інформацією, було максимально повним, а відомості, що надходять другим типом каналів, лише доповнювали інформацію офіційних каналів.

За таких умов постає проблема переведення інформації з неофіційних каналів комунікації в офіційні [253]. Пов'язано це ще й з тим, що невдоволення ступенем своєї безпеки, гострота небезпек, що загрожують інтересам людей, незадоволеність формами і методами забезпечення своєї безпеки і багато іншого, що відноситься до безпеки об'єктів і діяльності суб'єктів щодо її забезпечення, набувають форму нарікання та невдоволення. Офіційні ж канали нерідко несуть інформацію неабияк проціджену, яка часто не зовсім відповідає реальному стану справ у сферах безпеки суспільства та особи. Гірше, якщо офіційні канали з яких би не було причин не функціонують (навіть тимчасово). Наприклад, у зоні проведення військової операції на Сході України відсутність офіційної інформації породжувала найбезглуздіші чутки, які сприймались за щиру правду.

Усе згадане доводить, що навіть нормальна практика політичного керівництва й державного управління може свідчити про певний розрив між офіційними та неофіційними комунікаціями, адже офіційні канали мають головним чином галузевий або спеціалізований характер і з усього обсягу інформації обирають лише вузькопрофільну, що відповідає їм за

призначенням. Ураховуючи, що комплексність забезпечення нацбезпеки продовжує підвищуватися, вузькогалузевий спосіб вибору і передання інформації стає менш привабливим та й не зовсім ефективним. Слід ураховувати й той факт, що в міжгалузевих комунікаційних розривах губиться дуже цінна і дефіцитна інформація.

Крім того, структура офіційних каналів комунікації має тенденцію до старіння, відстаючи від нових вимог, ігноруючи нові соціально значущі зв'язки й нові потоки інформації. Нерідко спостерігається така тенденція: спочатку будь-яка нова інформація циркулює в неофіційних каналах комунікації і лише згодом, іноді із запізненням або зі спотворенням, потрапляє в офіційні канали, де готуються й ухвалюються рішення.

Слід наголосити, що розроблення та реалізація політики безпеки, насамперед її концептуальних і доктринальних засад, є процесом складним і комплексним. У дійсно правових державах він здійснюється на демократичній основі, до нього залучаються фактично всі сили, з яких складається політична організація суспільства: державні інститути (органи виконавчої та законодавчої влади, президент, силові структури держави, зовнішньополітичні відомства тощо), різноманітні недержавні організації (політичні партії, громадські об'єднання та організації, різні групи, зокрема тиску й підтримки, тощо), а також засоби масової інформації та комунікації.

Таким чином, інформаційне забезпечення нацбезпеки в цьому сенсі покликане забезпечити рівною мірою і доступ до інформації різним політичним партіям, і їх рівноважний інформаційний вплив на органи державної влади та державного управління.

Є підстави вважати, що для забезпечення найбільш повної інформації жорстка централізація її потоків (тільки через офіційні канали) виявляється недостатньо ефективною. Критикуючи неефективність такої централізації, М. Кроз'є в межах організаційно-комунікаційної концепції підкреслював: «Справжній сенс цієї централізації полягає у встановленні непроникного

екрана між тими, хто має право приймати рішення, і тими, інтереси яких вони зачіпають» [341].

Тож, для інформаційного забезпечення національної безпеки недостатньо самої лише науково-технічної революції. Необхідна ще така інформаційна революція, яка б створила умови для незрівнянно більш вільного переливу інформації з неофіційних каналів комунікацій в офіційні, державно-управлінські канали. Без цього розрив між кількістю інформації, що циркулює у сфері національної безпеки, та реально використовуваної, яка забезпечує ухвалення досить ефективних рішень у цій галузі, лише збільшуватиметься.

1.3. Методологічні чинники формування сучасного інформаційного суспільства в умовах викликів і загроз глобальному світу

Як ми вже зазначали раніше, характерною особливістю сучасного суспільства є перехід у якісно новий стан – перетворення його на так зване інформаційне суспільство, де відбувається активне проникнення нових інформаційно-комунікаційних технологій на всі сфери суспільного життя і загальне зростання їх впливу. Перехід до суспільства цього нового типу з різними інтенсивністю та результативності відбувається в усьому світі, і Україна не стала винятком. Нові технології не лише продовжують дедалі активніше впроваджуватися у промисловому виробництві, а і почали відігравати головну роль, як у ньому, так і в багатьох інших життєвих сферах, зумовлюючи відповідну державно-управлінську й економічну динаміку, водночас комп’ютери і мобільні телефони, насамперед завдяки мережі Інтернет, так глибоко увійшли у повсякденне життя більшості людей, що без них багато хто його світу просто не уявляє [83].

Унаслідок нової інформаційної революції, появи нових інформаційно-комунікаційних технологій, реклами сучасного способу життя в ЗМІ та за допомогою інших комунікативних засобів, комп’ютеризації освіти,

поширення електронних пристроїв, що забезпечують комфорт і зручність у повсякденному житті технокультурне середовище буденного життя зробилося вкрай мінливим [39].

Як зазначають автори колективної монографії «Інформаційна складова державної політики та управління» те, що людство ввійшло в стан інформаційного суспільства, фактично вимагає переосмислення всіх старих уявлень про інформацію, зокрема як про важливий інститут, адже сьогодні публічна сфера не може функціонувати, не враховуючи інформаційно-комунікативні процесів, які виступають не лише сполучною ланкою державної та політичної системи, а й необхідною умовою існування сучасного суспільства, де без розуміння сприйняття інформації, обміну та її тлумачення, тобто інформаційної взаємодії у загальному сенсі, вони не зможуть здійснювати свої політичні ролі [41, с. 9]

На наш погляд, процес глобальної інформатизації суспільства, який відбувається сьогодні, докорінно змінює звичний уклад життя і професійної діяльності мільйонів людей у всіх країнах світу.

Історія розвитку цивілізації зазнала вже не одну інформаційну революцію, якщо розуміти під такою докорінне перетворення відносин у суспільстві, зумовлене кардинальними змінами у галузі обробки інформації. Наслідком останньої такої революції стало висунення на перший план інформаційної індустрії – галузі, яка раніше не існувала, пов’язаної з виробництвом технічних засобів, методів і технологій для продукування нових знань. Її головною складовою є інформаційна технологія [123, с. 70–72].

Масштабні соціокомунікативні та соціокультурні трансформації суспільства у кінці XX ст.. та на початку XXI ст. стали предметом серйозного аналізу [367]. Тому наукова думка сформувала низку теоретичних концепцій, які пояснюють суть і спрямованість трансформацій соціуму, що відбуваються [320].

Щодо класифікацій цих теорій існують різні точки зору. На наш погляд, основні теоретичні підходи, які розглядають соціальні зміни в умовах розвитку інформаційних технологій, логічно об'єднати у такі три групи:

1) теорія інформаційного суспільства (Д. Белл, Е. Тоффлер, З. Бжезинський, М. Кастельс);

2) постклассична соціальна теорія (Г. Дебор, М. Маклюен, Ж. Бодрійяр);

3) теорія віртуалізації (А. Бюль, А. Крокер, М. Вейнстейн, М. Паетау).

Зазначені концепції можна умовно поділити на «оптимістичні», або концепції розвитку (теорія інформаційного суспільства), автори яких говорили про прогресивний розвиток масової свідомості в умовах інформаційного суспільства, і «песимістичні», або концепції змін (пост класична соціальна теорія і концепція віртуалізації), що роблять акцент на негативному й руйнуючому впливі інформаційних технологій на свідомість людини і соціальну взаємодію.

На наш погляд, методологічно цінним цей підхід робить те, що він чітко диференціює різні теорії відповідно до спрямованості їх остаточних висновків: «оптимістичні» і «песимістичні». Це оптимізує теоретико-методологічні побудови авторів, які аналізують соціальні зміни в умовах розвитку інформаційних технологій.

Однак, якщо в 1960-і рр. ідеї інформаційного суспільства мали характер чогось на кшталт футурологічних прогнозів, то в процесі вдосконалення електронної техніки й цифрових технологій більшість з передбачених теоретиками подій реально відбулося, а прогнози втілитись у життя, що виразилося в бурхливому розвитку ЗМІ, насамперед телебачення, створенні й широкому розповсюдженні персональних комп'ютерів, побудові глобальних інформаційних мереж, появі технологій віртуальної реальності та в інших технологічних інноваціях.

Усі ці досягнення разом узяті надзвичайно сильно змінили людське життя, не лише висунувши у суспільстві на перше місце інформаційну діяльність, тобто діяльність, пов'язану з виробництвом, споживанням,

трансляцією, зберіганням і захистом інформації, а й ускладнивши та перетворивши світ таким чином, що традиційних підходів для його пізнання й осмислення виявилось замало [138].

Тому виглядає цілком правомірним підхід, коли виділяються три етапи розвитку наукових теорій інформаційного суспільства. На першому етапі – з кінця 1950-х і приблизно до середини 1960-х рр. – почалося осмислення того, що технологічні чинники розвитку починають превалювати над політичними, соціальними та, на наш погляд, державно-управлінськими.

Ця теорія отримала назву «теорії постіндустріального суспільства» і вперше була введена в науковий обіг американським соціологом Д. Рісменом у 1958 р Це був період накопичення інформації та ідей щодо майбутнього суспільства [323].

Другий період датується серединою 1960-х – кінцем 1980-х рр. Його умовно можна назвати футурологічним, оскільки в дослідженнях головним чином йшлося про майбутній тип суспільства. цей етап пов’язано з працями таких учених, як Д. Белл, З. Бжезинський, Р. Катц, М. Маклюен, Е. Масуда, М. Порат, Т. Стоуньер, Е. Тоффлер та ін.

І, нарешті, третій період вивчення інформаційного суспільства почався з 1990-х рр. Цей етап розвитку досліджень пов’язується, перш за все, з іменами П. Дракера та М. Кастельса [134, с. 20–22]. На наш погляд, методологічними перевагами цієї концепції є її спирання на порівняльно-історичний метод. Зокрема, у концепції розкривається логіка розгортання теорій постіндустріального, а потім – інформаційного суспільства, робиться акцент на історії послідовного висунення різних теорій. Саме історія виникнення та розвитку різних теоретичних концепцій надає можливість глибше осмислити той соціальний контекст, в умовах якого вони створювалися [336].

Отже, наукова думка констатувала наявність передумов серйозних соціокомунікативних, соціокультурних та державно-управлінських трансформацій суспільства ще в кінці 1950-х рр. Створена в цей період часу

концепція постіндустріального суспільства стала по-своєму першою науковою конструкцією, що охоплює техніко-технологічні зміни суспільства другої половини XX ст.

Із середини 1960-х рр. Д. Белл, Д. Рісман, О. Тоффлер, А. Турен та інші вчені порушують проблему переходу найрозвиненіших країн в якісно іншу стадію соціального розвитку, яку згадані вчені характеризують як постіндустріальне, або інформаційне суспільство, головною визначальною особливістю (критерієм) якого є ключова роль інформаційних технологій у діяльності та розвитку людей і людства.

Одним із центральних елементів теорії постіндустріального суспільства виступає технологічний детермінізм. Феномен НДР (наукові дослідження і розробки; за своєю суттю – фактичний вияв об'єднання науки, техніки та економіки), на думку Д. Белла, відіграватиме дедалі важливішу роль у суспільстві, націленому на майбутнє [26; 338].

Орієнтованість, спрямованість у майбутнє є ще однією важливою особливістю постіндустріального суспільства. Вона передбачає контроль за технологіями, їх оцінювання та розробку моделей технологічного прогнозу. Крім того, ще однією істотною характеристикою постіндустріального суспільства, вважає Д. Белл, є нова інтелектуальна технологія, що застосовується для ухвалення управлінських рішень (на нашу думку, наразі головним чином рішень державно-управлінського характеру), тобто рішень, які ухвалюють органи державної влади [26].

Крім того, дослідник стверджував, що нова інтелектуальна технологія ще до кінця XX ст. почне відігравати таку ж само значну роль у людських справах, як машинна технологія за минулі півтора століття. Ця технологія, за словами Д. Белла, передбачає замість інтуїтивних суджень використання алгоритмів як правил вирішення проблем, які можна реалізувати навіть в якомусь автоматі, в комп'ютерній програмі чи в низці інструкцій, що ґрунтуються на певних математичних формулах. Тобто інтелектуальна технологія є пов'язаною з використанням математичної (статистичної) або

логічної техніки під час роботи з «організованою складністю», прикладом якої можуть слугувати різні, серед іншого соціальні, системи й організації [338].

На відміну від індустріального суспільства, в якому головний конфлікт між працею і капіталом обумовлюється зосередженістю власності в руках капіталістів, у постіндустріальному суспільстві таким виступає боротьба між знанням і некомпетентністю. Зауважимо, що вже наприкінці 1960-х рр. ця концепція була піддана критиці з боку «нових лівих», які побачили в ній не нову стадію суспільного розвитку, а ідеалізований варіант капіталістичного суспільства.

Водночас навіть прихильники постіндустріальної теорії відзначають методологічну складність чіткого визначення окремих типів суспільства, тим більше їх хронологічних меж. Постіндустріальному суспільству навряд чи може відповідати чітка дефініція, заснована на одному або хоча б на незначній кількості базових характеристик. Сучасний соціальний прогрес не є заданим і керованим процесом [357].

У кінці 1960-х – на початку 1970-х рр. значної популярності в наукових колах набуває концепція інформаційного суспільства. У найзагальніших рисах інформаційне суспільство можна визначити як такий суспільний устрій, головним чинником розвитку якого стає створення і використання індустрії інформації (комп'ютерів, мікроелектроніки, комунікаційно-обчислювальних мереж, національних і міжнаціональних баз даних), тобто це різновид теорії постіндустріального суспільства.

Автором однієї з найцікавіших концепцій інформаційного суспільства був японський вчений Е. Масуда, який прагнув зрозуміти прийдешню еволюцію соціуму. Дослідник одним із перших у світі обґрунтував концепцію інформаційного суспільства як логічного розвитку теорії постіндустріального суспільства. У своїх працях він висловив мрію про «суспільство, в якому буде процвітати людська інтелектуальна творчість, а не рясне матеріальне споживання» [357].

В його роботі «Інформаційне суспільство як постіндустріальне суспільство» висвітлено такі принципи «композиції» майбутнього суспільства: «основою нового суспільства буде комп'ютерна технологія з її фундаментальною функцією заміщати або посилювати розумову працю людини; інформаційна революція буде швидко перетворюватись на нову продуктивну силу й уможливить масове виробництво когнітивної, систематизованої інформації, технології і знання; провідною галуззю економіки стане інтелектуальне виробництво, продукція якого буде акумулюватись, а акумульована інформація стане поширюватися через синергетичне виробництво і пайове використання» [357].

Учений пропонує нову, цілісну й привабливу своєю гуманністю утопію XXI ст., ним самим названу «комп'ютопією», яка полягає в такому:

1) вибір напрямку реалізації цінностей часу;

2) свобода ухвалення рішення і рівності можливостей;

3) розквіт різних вільних спільнот;

4) синергетичний взаємозв'язок у суспільстві;

5) функціональні об'єднання, вільні від надуправляючої влади.

«Нове суспільство потенційно матиме можливість досягти ідеальної форми суспільних відносин, оскільки функціонуватиме на основі синергетичної раціональності, яка і замінить принцип вільної конкуренції індустріального суспільства» [357].

М. Кастельс також належить до найяскравіших сучасних теоретиків інформаційного («мережевого») суспільства. Його концепція ґрунтується на розумінні інформації як основи соціальної організації. Зростаючі оперативність, мобільність і гнучкість, які торкнулися всіх сфер людської життєдіяльності, роблять природним перехід до мережевих форм соціальної організації: мережеве підприємство в економіці, інтерактивна політична система, єдина інформаційна мережа Інтернет.

На думку М. Кастельса, інформація є тим ресурсом, який легше за інші долає усілякі перешкоди і кордони. Інформаційну еру він розглядає як епоху

глобалізації, а мережеві структури – водночас і як засіб, і як результат глобалізації суспільства. «Саме мережі, – зазначає дослідник, – створюють нову соціальну морфологію наших суспільств, а поширення “мережевої” логіки суттєво відбивається на перебігу та результаті процесів, пов’язаних з виробництвом, буденним життям, культурою та владою» [134, с. 494].

Одна з теорій виникнення інформаційного суспільства представляє еволюцію інформаційної структури людської цивілізації у вигляді спіралі, що звужується, зі змінним кроком, побудованої у тривимірному просторі, в координатах інформації і з введенням параметрів часу і прогресу.

Об’єктивними й безпосередніми приводами виникнення інформаційного суспільства вчений вважає швидке зростання ролі інформаційних ресурсів і комунікацій у житті суспільства. Це зростання обумовлене революцією, що відбулась у сфері інформаційних технологій і призвела до різноманітних наслідків: від появи нових професій і серйозної зміни соціальної структури суспільства до виникнення нових стилів у міській архітектурі [357].

Водночас концепція інформаційного суспільства породжує чимало критичних зауважень. Так, Ф. Уебстер відзначає: «хоча як евристичний термін “інформаційне суспільство” має певну цінність для дослідження основних характеристик сучасного світу, все ж він надто не точний, щоб прийняти його як наукову дефініцію». Автор указує, що саме базове поняття цього суспільства до певного моменту було корисним, бо надало можливість додати організацію до явищ, які підлягали дослідженню. Серед іншого саме концепція інформаційного суспільства допомогла науковцям розглядати різноманітні явища водночас і самі по собі, і в їх у сукупності (наприклад, зміни в структурі зайнятості чи у сфері освіти, виникнення нових засобів поширення інформації тощо). Однак, на думку Ф. Уебстера, хоча на певному етапі поняття «інформаційне суспільство» відіграло позитивну роль, воно «вводить в оману, особливо тим, що натякає на існування нового типу

суспільства, де соціальні зміни повністю визначаються як наслідки етапів інформаційної революції» [305, с. 14].

Втім, на наш погляд, у сучасному суспільстві наслідки науково-технічного прогресу та інформаційної революції є очевидними. Як зазначає низка авторів, «стрімкий розвиток і поширення нових інформаційно-комунікаційних технологій унаслідок науково-технічного прогресу набуває сьогодні характеру безпрецедентної за своїми масштабами інформаційної революції, яка дедалі сильніше впливає на політику, економіку, науку та інші сфери життєдіяльності суспільства як у межах національних кордонів, так і загалом у світі. Інформація та знання стають одним із стратегічних ресурсів держави, масштаби використання якого досягли зіставних з використанням традиційних ресурсів, а доступ до них став одним з головних чинників соціально-економічного розвитку. Роль цього чинника, що постійно посилюється, як засобу прискорення темпів глобальної інтеграції в економіці та інструменту впливу на масову свідомість, культуру і міжнародні відносини надає можливість говорити про те, що в останній чверті XX ст. людство вступило в нову стадію свого розвитку – в епоху інформаційного суспільства» [188; 304].

Російський науковець Д. Іванов констатує: «комп'ютеризація всіх сфер суспільної діяльності й повсякденного життя людини – найбільш вражаючий феномен останньої чверті XX ст. У найрозвиненіших країнах – США, Німеччині, Великобританії, Японії – кількість комп'ютерів на тисячу жителів досягла до кінця 1990-х рр. рівня 250–400 одиниць. Крім кількісного зростання, велике враження на будь-якого аналітика справляє зростання кількості функцій – способів застосування комп'ютерних технологій. Зі звичайної обчислювальної машини, що зветься нині напівзабутою абревіатурою ЕОМ, комп'ютер перетворився на універсальний пристрій, який з однаковим успіхом може слугувати професійним інструментом ученого, інженера, бізнесмена, юриста чи лікаря, а також засобом навчання, повсякденного спілкування, розваги» [114]. У зв'язку з цим, на нашу думку,

очевидно, що в сучасному суспільстві комп'ютерна віртуальна реальність є особливим типом комунікативного середовища, в якому відбувається віртуальне спілкування.

У сучасних умовах основним сенсоутворюючим елементом формування інформаційного суспільства є не інформація, а комунікація, «людська складова» в її соціально-гуманістичному значенні.

Віртуальний характер спілкування, на нашу думку, докорінно змінює становище людини в соціумі і значно трансформує її свідомість. Сучасне інформаційне суспільство в процесі глобалізації, відкритого інформаційного взаємообміну, поступової трансформації духовно-особистісних особливостей, обумовлених інституціональним характером суспільної системи національної держави, створює перспективу істотної зміни положення людини, готовності до сприйняття нових цінностей, активізації особистісного начала, самовизначення.

Виходячи з вищевикладеного, стає очевидним, що розвиток інформаційно-комунікаційних технологій на певному етапі призводить до виникнення ефекту «віртуалізації» соціуму. Перші спроби створення моделей сучасності, які спирались на об'єктивні передумови формування віртуального суспільства, були зроблені наприкінці XX ст. одночасно в Німеччині (А. Бюль і М. Паетау) і в Канаді (А. Крокер і М. Вейнстейн).

З погляду теорії «віртуального суспільства» А. Бюля, з розвитком технологій віртуальної реальності комп'ютери з обчислювальних машин перетворились на універсальні машини, що продукують «дзеркальні» світи. У кожній підсистемі суспільства вникають «паралельні» світи, де функціонують віртуальні аналоги реальних механізмів відтворення суспільства: економічні інтеракції та політичні акції в мережі Інтернет, спілкування з персонажами комп'ютерних ігор тощо. Цей процес, за якого завдяки комп'ютерним технологіям реальний простір як місце відтворення суспільства заміщується іншим – віртуальним – простором, А. Бюль назвав «віртуалізація» [257].

Західні вчені А. Крокер і М. Вейнстейн зосередились на критиці – викритті кіберкапіталізму, побачивши у ньому систему, що створює новий тип нерівності й експлуатації. Вони розглядають власників компаній, що виробляють програмне забезпечення та надають доступ в Інтернет, як ядро нового панівного класу, що прагне віртуальності й перетворює віртуальну реальність на капітал. Під віртуалізацією А. Крокер і М. Вейнстейн розуміють новий тип відчуження – відчуження людини від власної плоті в процесі користування комп'ютерами та перетворення її на потоки електронної інформації, які підживлюють віртуальний капітал [114].

Спеціаліст з інформаційного суспільства М. Паетау вважає появу гіперпростору глобальної мережі Інтернет наслідком «використання» суспільством нових форм комунікації для самовідтворення «аутопойесіса» (за термінологією Н. Лумана). Разом із традиційними формами, «реальними» інтеракцією та організацією комунікація за допомогою комп'ютера долучається до створення соціальності. Зміну суспільства цей науковець інтерпретує як структурну диференціація системи через появу в ній нових елементів – віртуальних аналогів реальних комунікацій [114].

На думку М. Кастельса, «у віртуальному суспільстві індивіди виступають не лише такими, що пасивно сприймають інформацію, а й є активними творцями нових цінностей, моделей поведінки, які вони втілюють в реальному житті. Людина і раніше могла, причому досить легко, потрапити у віртуальний світ, наприклад, занурюючись у споглядання картини, кінофільму або просто захоплено читаючи книгу. Однак у всіх подібних випадках активність людини була обмежена її позицією глядача або читача, або слухача, вона сама не могла включитися в процес як активний член. Зовсім інші можливості надають віртуальні системи: самому включитися в дію, причому часто не лише в умовному просторі й світі, але й як би в цілком реальному, в усякому разі, з точки зору сприйняття людини» [339].

Впровадження комп'ютерних технологій в соціальну сферу призводить до посилення її символічності. Формування гіперсимволічної реальності

стало предметом наукового аналізу таких постмодерністів, як Ж. Бодрійяр, Ж. Дельоз та Ж. Ф. Ліотар (концепції симулякрів).

Так, значний внесок у вивчення цієї проблеми зробив французький вчений Ж. Бодрійяр. У його теорії термін «симулякр» нерідко вживається для позначення артефактів віртуальної реальності. «Симулякр – (в пер. з фр. – стереотип, псевдоріч, порожня форма) – образ відсутньої дійсності, правдоподібна подоба, позбавлена першотвору, поверхневий, гіперреалістічний об'єкт, за яким не стоїть будь-яка реальність. Це марна форма, самореференційний знак, артефакт, заснований лише на власній реальності» [91].

Ж. Бодріяр вважає, що в сучасному суспільстві порушується зв'язок взаємодії з реальністю [91]. Виникає явище гіперреальності (симуляції чого-небудь). Вона більш приваблива, ніж реальність, з якою ми стикаємося в повсякденному житті. Наприклад, створюване пропагандою уявлення про досягнення в тій чи іншій сфері є більш вражаючим, ніж у реальному житті.

Отже, реальна взаємодія витісняється симулякрами – знаками або образами, що відриваються за змістом від конкретних об'єктів, явищ, подій і виступають як фальсифікації, які не відповідають оригіналу. Тим самим утверджується ілюзія реальності. Наприклад, видимість виборів замінює демократію, мильні опери – любов, «фабрики зірок» – справжнє мистецтво.

На нашу думку, можна погодитися з точкою зору про те, що зміст поняття «віртуальне суспільство» містить ознаки віртуальності в усіх сферах суспільства. Воно пов'язує віртуалізацію не тільки з технічними, але й із соціальними трансформаціями, що відбуваються в суспільстві.

Д. Іванов зазначає: «і хоча термін "віртуальне суспільство" часто пов'язують з комп'ютерної сферою, проте зараз все частіше це поняття вживається в контексті, що повністю виходить за межі сфери інформатики та комп'ютерної техніки. Глибина проникнення віртуальності в соціальне й індивідуальне життя надає можливість говорити про "віртуалізацію"

суспільства. На нинішньому етапі інформаційні технології починають виступати у своїй віртуальній іпостасі» [114].

Отже, незважаючи на відмінності в позиціях учених, які займаються проблематикою постіндустріального, інформаційного суспільства (чи іншою, близькою за змістом), можна з упевненістю констатувати, що науково-технічна революція та широке впровадження інформаційно-комп'ютерних технологій призвели до істотних трансформацій суспільства.

Однак, як відомо, далеко не всі трансформації соціуму можна віднести до позитивних. Головна проблема в тому, що поширення інформаційно-комунікаційних технологій призводить до низки негативних соціальних ефектів, серед іншого віртуалізації реальності, симуляції соціальних взаємодій, інформаційної нерівності тощо, тому закономірним є, наприклад, питання про те, як тенденції глобалізації та інформатизації проявляють себе в українській державі.

У XXI ст. в Україні спостерігається бурхливий розвиток телекомунікаційних мереж, Інтернету та мобільного зв'язку. Впроваджуються нові інформаційні технології, розвивається комп'ютерна преса, відкриваються нові сайти, численні компанії пропонують послуги IP-телефонії, реалізовують стільникові телефони, комп'ютери, модеми тощо. Однак усі вищеописані процеси розвиваються досить стихійно, з незрозумілим поки що знаком для суспільства, з неясними й невизначеними наслідками [102; 152].

В Україні, на наш погляд, сьогодні не існує сформованої загальнонаціональної стратегії входження у глобальний інформаційний простір, не вироблені пріоритети, не сформульовані цілі, не усвідомлені альтернативи [331].

Зазначимо, що актуальність цього питання цілком усвідомлюється. Так, уже на початку XXI ст. активно проводилися конференції, «круглі столи», відкриті дискусії, де наукові, політичні, економічні актори прагнули

виробити цілі, підходи, стратегії щодо входження України у глобальне інформаційного суспільство.

З одного боку, в нашій країні є потужний науковий, культурний, освітній потенціал, адекватний інформаційному суспільству; з іншого – владні структури та ділові кола, що приймають ключові рішення, націлені на отримання швидкого надприбутку, одержуваного за рахунок надексплуатації природних ресурсів.

У цій ситуації розвиток інформаційної сфери суспільства та інноваційного сектора економіки та державного управління, заснованих на науковому потенціалі, штучно гальмуються. Разом із ними гальмується й розвиток українського суспільства в цілому.

На наш погляд, абсолютно очевидно, що багато пострадянських країн, і Україна не виняток, відстають у розвитку інформаційно-комунікаційних технологій і, відповідно, характеризуються певним «запізненням» у процесі інтеграції в структури інформаційного суспільства.

Сучасне інформаційне суспільство, на наш погляд, повинно являти собою єдину комп'ютеризовану інформаційну спільноту людей, діяльність яких головним чином зосереджена на обробці інформації, де матеріальне виробництво і виробництво енергії автоматизовано, а інформаційні технології набувають глобального характеру, охоплюють усі сфери людської діяльності.

Унаслідок проникнення, поширення та розвитку інформаційних і телекомунікаційних технологій і всеосяжного охоплення інформаційними технологіями всіх сфер життя суспільства відбуваються зміни суспільного виробництва, дозвілля соціальних груп, виховання індивідів, а також соціальної структури суспільства, економічних і державно-управлінських відносин. Завдяки глобальній інтернет-мережі людина отримує можливість брати активну участь у політичному, державному, економічному, освітньому, соціальному тощо житті суспільства.

Водночас завдячуючи Інтернету інтенсифікуються процеси глобалізації та інформатизації соціуму. Наразі є сенс говорити про феномен глобального електронного середовища. Це у свою чергу створює певні загрози існуванню держав, перш за все в інформаційній сфері.

На нашу думку, основними чинниками, що впливають на формування електронного середовища, є:

– трансформація соціальних і державно-управлінських інститутів в умовах розвитку інформаційного суспільства;

– розвиток онлайнових співтовариств, їх взаємодія між собою і традиційними громадами;

– вплив розвитку Інтернету на зміну системи соціальної комунікації та забезпечення інформаційної безпеки держави;

– трансформація сучасної освіти, розвиток дистанційної освіти;

– проблема збереження культурної ідентичності;

– формування «електронної економіки»;

– формування «електронного уряду» і в кінцевому підсумку – «формування механізмів електронного уряду».

Отже, можна зробити низку висновків. Так, протягом другої половини XX ст. сформувалися кілька теоретичних концепцій, що описують характер і спрямованість соціокомунікативних, соціокультурних і, як ми вже вказували, державно-управлінських трансформацій суспільства. Одна частина концепцій характеризується позитивною оцінкою змін, що відбуваються (теорія інформаційного суспільства), а інша – негативною, з акцентом на негативні аспекти глобалізації та інформатизації соціуму (постклассична соціальна теорія і концепція віртуалізації, що несуть загрози державі в контексті інформаційної безпеки).

Незважаючи на високий теоретико-методологічний рівень зазначених теоретичних концепцій, усе ж таки залишається чимало «білих плям» у пізнанні нової інформаційно-комунікаційної реальності. Зокрема, слабким місцем усіх концепцій є вузькість бази їх наукового аналізу. Матеріалом для

наукових узагальнень насамперед стала ситуація в індустріально розвинених країнах (в Японії, США, Німеччині тощо).

У сучасному світі спостерігається значне розшарування щодо використання інформаційно-комп'ютерних технологій. Так, за цим показником суттєво відстають країни Африки. Склалася неоднозначна ситуація і в пострадянських країнах, зокрема в Україні, де спостерігається значний цифровий розрив між регіонами. Характер інтеграції України у глобальний інформаційний простір є досить суперечливим. Так, завдяки економічній глобалізації українським організаціям, компаніям і громадянам стали доступними всі сучасні розробки у сфері інформаційно-комунікаційних технологій. Водночас з іншого боку, за справедливим зауваженням М. Кастельса, багато пострадянських країн, серед них і Україна, все ще відчувають наслідки того науково-технологічного відставання від провідних країн, що намітився ще в 1990-і рр. У результаті відзначається нерівність можливостей у сфері «високих технологій» і негативні наслідки інформаційної асиметрії, що позначаються в різних сферах і насамперед у системі безпеки держави [339].

Висновки до першого розділу

Підбиваючи підсумки викладеному, підкреслимо головні висновки. Так, інформаційне забезпечення національної безпеки можна вважати процесом задоволення інформаційних потреб суб'єктів національної безпеки. Воно відіграє важливу та багатопланову роль у:

– визначенні національних інтересів і пріоритетів нацбезпеки;

– пошуку нових форм і способів її забезпечення;

– впливі на діяльність суб'єктів безпеки, формування їхніх поглядів і поведінки відповідно до визначених пріоритетів і цінностей розглядуваної сфери;

– розвитку загального механізму ухвалення та реалізації державно-управлінських рішень у сфері нацбезпеки.

Якісна характеристика інформаційного забезпечення такої безпеки визначається не лише вибором форм, методів і способів його здійснення, а і специфікою та особливостями його реалізації в конкретній країні.

Конкретний зміст інформаційного забезпечення національної безпеки залежить від характеру інформаційних потреб суб'єктів нацбезпеки, а також форм, видів і способів їх задоволення.

Вивчення та оптимізація інформаційних зв'язків і потоків, що циркулюють у сфері нац безпеки, умов і чинників, які впливають на рух інформації, є важливими складовими змісту інформаційної діяльності у розглядуваній сфері.

Отже, можна стверджувати, що в сучасному суспільстві відбуваються значні соціокомунікативні, соціокультурні та державно-управлінські трансформації. Цей процес розпочався ще у другій половині XX ст. і здійснюється у різних країнах з різним ступенем інтенсивності. Цілком очевидно, що всілякі системи, побудовані на основі мікропроцесорних технологій, комп'ютерних мереж, інформаційних технологій, телекомунікаційного зв'язку та Інтернету, виступають матеріально-технологічною базою інформаційного суспільства, що забезпечує рух інформаційних потоків і в кінцевому підсумку суттєво впливає на інформаційне забезпечення держави у сфері безпеки.

РОЗДІЛ 2
КОНЦЕПТУАЛЬНІ ПІДХОДИ ЩОДО ОСОБЛИВОСТІ ФОРМУВАННЯ БЕЗПЕКИ ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ

2.1. Процес інформатизації державно-управлінських відносин у формуванні державної безпеки в умовах глобального інформаційного суспільства

Глобалізація стала найважливішою тенденцією світового розвитку кінця XX – початку XXI ст. Ця тенденція чітко проявляється в державно-управлінській, економічній, соціальній, політичній, ідеологічній і культурній сферах. Останніми роками в цьому контексті найбільшої актуальності набуває інформаційна сфера, яка у зв'язку з бурхливим розвитком інформаційно-комунікаційних технологій, появою принципово нових і високоефективних методів інформаційного обміну та впливу стає важливим інструментом державно-управлінських і політичних перетворень.

В умовах постійно мінливого світу стає очевидним, що використання сучасних інформаційних технологій безпосередньо впливає і на інформаційну безпеку держави. Як справедливо зазначав відомий американський футуролог О. Тоффлер, на сучасному етапі знання і інформація стали найважливішими ресурсами влади [304, с. 46].

У сучасному світі відбувається інтенсивне нарощування інформаційно-комунікаційного потенціалу, все активніше фахівцями в області інформаційних комунікацій сучасний етап називають інформаційною глобалізацією. На наш погляд, не менш точною характеристикою змін, що відбуваються у XXI ст. у розвитку сучасних держав, є формування глобального інформаційного суспільства, в якому

інформаційні ресурси державного управління набувають найбільш важливого значення поряд з ресурсами сили і багатства.

Основним підґрунтям для цього виступає розвиток комунікацій, використання космічного простору для передачі інформації, зростання глобальних інформаційних мереж, комп'ютеризація багатьох процесів життєдіяльності людства [339].

Сьогодні багато експертів у галузі державно-управлінських, економічних і політичних відносин зазначені вище фактори відносять до поняття «інформаційне суспільство». При цьому слід мати на увазі, що багато вчених у галузі суспільних відносин наразі не дійшли єдиного розуміння змісту цього поняття. Одні вважають, що це – суспільство, в якому забезпечується легкий і вільний доступ до інформації по всьому світу, інші – це суспільство, в якому основними об'єктами й результатами праці більшості є інформація і знання.

Найбільшу підтримку серед дослідників отримало визначення інформаційного суспільства як такого, де основним предметом праці більшості громадян є інформація і знання, а знаряддям праці й управління – інформаційні технології.

Більш розгорнуто інформаційне суспільство може бути охарактеризоване як фаза розвитку сучасної цивілізації, для якої характерно різке підвищення ролі інформації і знань у житті суспільства, зростання частки інформаційних комунікацій, інформаційних продуктів і послуг у валовому внутрішньому продукті (ВВП), створення глобального інформаційного простору, що забезпечує ефективне інформаційну взаємодію людей, їх доступ до світових інформаційних ресурсів і задоволення їх соціальних і особистих потреб в інформаційних продуктах і послугах [189; 191].

З точки зору теорії управління, зокрема марксистського підходу, який акцентує роль впливу продуктивних сил на структуру виробничих відносин, інформаційне суспільство можна визначити як таке, в якому

основним предметом праці більшої частини людей є інформація і знання, а знаряддям праці – інформаційні технології.

Суспільні відносини будуть багато в чому визначаються саме цими обставинами. Відповідно економіка, державне управління в суспільстві будуть орієнтовані на виробництво, насамперед продуктів інформаційної та інтелектуальної діяльності, пов'язаних із продукуванням нової інформації та нових знань, доведенням їх до вигляду, зручного для споживання іншими людьми, та реалізацією (зокрема продажем) цих продуктів.

Основними характерними рисами інформаційного суспільства є інформаційна економіка та інформаційне управління, високий рівень інформаційних потреб усіх членів суспільства й фактичне їх задоволення для основної маси населення, висока інформаційна культура, вільний доступ кожного члена суспільства до інформації, обмежений тільки інформаційною безпекою особи, суспільних груп і держави.

Якщо говорити більш конкретно, то інформаційному суспільству притаманні такі ознаки:

– наявність єдиного інформаційного простору;

– домінування в економіці й публічному управлінні нових технологічних укладів, що базуються на масовому використанні інформаційно-комунікаційних технологій [340];

– підвищення ролі інфраструктури (телекомунікаційної, транспортної, організаційної) в системі суспільного виробництва, державного управління, а також посилення тенденцій до спільного функціонування в економіці та управлінні інформаційних і грошових потоків;

– зростання значущості проблем забезпечення інформаційної безпеки особи, суспільства і держави, наявність ефективної системи забезпечення прав громадян і соціальних інститутів на вільне отримання, розповсюдження і використання інформації;

– високий рівень освіти, зумовлений розширенням інформаційного обміну на міжнародному, національному та регіональному рівнях, і відповідно підвищена роль кваліфікації, професіоналізму і здібностей до творчості як найважливіших характеристик праці;

– провідна роль інформаційних ресурсів у забезпеченні сталого поступального розвитку суспільства і забезпечення інформаційної безпеки держави;

– фактичне задоволення потреб суспільства в інформаційних продуктах і послугах.

У сучасному світі відбувається усвідомлення того, що інформація є необхідною умовою будь-якої доцільної діяльності. Найбільший економічний, соціальний і державно-управлінський успіх сьогодні супроводжує ті країни і регіони, які активно використовують сучасні засоби інформаційно-комунікаційних технологій [192; 340]. Доступна для оперативного відтворення засобами комп'ютерної обробки інформація перетворюється на найважливіший фактор соціального розвитку суспільства, стає стратегічним ресурсом поряд з традиційними – матеріальними та енергетичними і здатна захистити державу від усього різноманіття інформаційних загроз і викликів сучасного глобалізованого світу.

Найважливішою особливістю інформаційного суспільства є перенесення акценту у виробництві з використання сировини, матеріалів та енергії на продукування інформації й надання інформаційних послуг. Як зазначав відомий японський вчений І. Масуда, саме «продукування інформаційного продукту, а не продукту матеріального буде рушійною силою освіти і розвитку суспільства» [357, с. 29].

В аспекті соціальних відносин слід говорити про те, що сучасний період розвитку людської цивілізації характеризується істотною зміною характеру основних соціальних процесів і відрізняється прагненням розвиненого індустріального суспільства до вдосконалення своїх

соціальних структур та інститутів. Вивчення цих процесів змушує і вчених, і політиків робити висновки про те, що людство має справу з останніми досягненнями науково-технічного прогресу як з фактором постіндустріального соціально-економічного розвитку в рамках сучасної цивілізації.

Сьогодні все більшої актуальності набуває питання про створення штучного інтелекту, що в сучасних умовах зовсім не виглядає фантастично. Це, у свою чергу, може глобально змінити всю систему управління суспільством і державою, сформує нові вимоги до системи інформаційної безпеки. Ключовими, на наш погляд, соціотехнічними умовами, що формують і спрямовують процеси постіндустріального розвитку, є свідоме й цілеспрямоване використання в економіці, соціальній практиці й системі державного управління, як ми вже зазначали вище, систем штучного інтелекту, і, зокрема, комп'ютерних інформаційно-комунікативних технологій, телекомунікацій і мережі Інтернет, модемного і факсимільного зв'язку, електронної пошти, нових технологій телевізійного мовлення, охоплення ними всього інформаційного простору держави.

Розширення сфер застосування технічних і технологічних інновацій породжує неоднозначні й нетривіальні форми державного, політичного і соціокультурного розвитку. У зв'язку з цим постіндустріальний етап у розвитку сучасної цивілізації характеризується якісно новими формами соціальної, економічної та державно-управлінської еволюції [352].

Провідною й багато в чому знаковою особливістю сучасного світу стає формування глобальної інформаційної індустрії, розвиток якої трансформує роль інформації і знань в соціально-економічному розвитку й впливає на свідомість і самосвідомість людини [151, с. 67]. Водночас місце і роль людини в сучасному світі стрімко змінюються.

Вперше у досить виразному вигляді ідея інформаційного суспільства була сформульована наприкінці 60-х – на початку 70-х рр. XX ст. Введення

в науковий обіг терміна «інформаційне суспільство» приписується професору Токійського технологічного інституту Ю. Хаяші [цит. за 2]. У ті часи інформаційне суспільство визначалося як таке, в якому процес комп'ютеризації надасть людям доступ до надійних джерел інформації, позбавить їх від рутинної праці, забезпечить високий рівень автоматизації виробництва.

Приділяючи значну увагу трансформації людських цінностей в інформаційному суспільстві, І. Масуда, глава Інституту інформаційного суспільства та один із авторів «Плану інформаційного суспільства», представленого Інститутом розробки використання комп'ютерів (JACUDI), висунув концепцію, згідно з якою інформаційне суспільство буде безкласовим і безконфліктним; це буде суспільство згоди з невеликим урядом і державним апаратом управління. Він писав, що, на відміну від індустріального суспільства, характерною цінністю якого є споживання товарів, характерною цінністю інформаційного суспільства буде час. У зв'язку з цим зростатиме й цінність культурного дозвілля [357].

У 1970-ті рр. відбулася конвергенція двох майже одночасно народжуваних ідеологій – інформаційного суспільства і постіндустріалізму. Остання, на відміну від першої, мала досить солідну теоретичну основу й універсалістську орієнтацію. Ідея постіндустріального суспільства була висунута ще в 1960-х рр. американським футурологом Д. Беллом, який у розгорнутому вигляді представив концепцію постіндустріалізму у книзі «Початок постіндустріального суспільства. Досвід соціального прогнозу», виданій у 1973 р. Концепція постіндустріалізму в її оригінальному варіанті, представленому в роботах Д. Белла, виявилася досить глибокою в теоретичному відношенні, цікавою в плані поставлених питань і відкрила широкі дослідницькі перспективи.

Варіант конвергенції ідей постіндустріалізму та інформаційного суспільства в дослідженнях Д. Белла представляє видана в 1980 р. монографія «Соціальні рамки інформаційного суспільства» [26].

Вираз «інформаційне суспільство» у Д. Белла – це нова назва для постіндустріального суспільства, що підкреслює не його положення в послідовності ступенів суспільного розвитку – після індустріального суспільства, а основу визначення його соціальної структури – інформацію. «У наступному столітті, – стверджував Д. Белл, – вирішальне значення для економічного та соціального життя, для способів виробництва знання, а також для характеру трудової діяльності людини набуває становлення нового соціального укладу, заснованого на телекомунікації [26].

У середині 1970-х рр. критичне ставлення до концепції постіндустріалізму виразилося, зокрема, в роботі французьких фахівців С. Нора і А. Мінка «Комп'ютеризація суспільства. Доповідь Президенту Франції». В інформаційному суспільстві, підкреслювали С. Нора і А. Мінк, групові плани більшою мірою, ніж раніше, відбивають соціальні та культурні устремління. Одночасно зростатимуть і зовнішні тиски. У цих умовах «тільки влада, що володіє належною інформацією, зможе сприяти розвитку і гарантувати незалежність країни [цит. за 318].

Аналізу й вивченню сучасного цивілізаційного розвитку та основних характеристик феномена інформаційного суспільства було присвячено чимало досліджень, серед яких необхідно виділити праці Д. Белла, М. Кастельс, Д. Лайона, Дж. Мартіна, І. Масуди, А. Тоффлера, Ф. Фукуями та Ф. Хайєка. Багато в чому саме їм належить заслуга з привернення уваги до характеристик соціального руху інформації і знань та затвердження уявлення про те, що конкретною формою самоорганізації життєдіяльності людини у світі сучасних технологій виступає інформаційне суспільство.

У межах запропонованих ними концепцій інформаційне суспільство в цілому розглядається як модель розвитку соціальних зв'язків і відносин, формування якої відбувається за рахунок досягнень «електронної

революції», а також швидкого розвитку обчислювальної техніки та інформаційно-комунікативних технологій.

Технократичний підхід до розуміння основних моментів соціального й державно-адміністративного процесу інформації і знань стає також визначальною умовою формування державної політики найбільш розвинених країн світу в галузі інформатизації й комп'ютеризації основних сфер життєдіяльності, багато в чому визначаючи спрямованість і зміст основних процесів глобалізації світової економіки та державного управління.

Разом із тим ускладнення соціотехнічних форм руху інформації і знань породжує, на наш погляд, непередбачуваність державно-управлінських, політичних і соціокультурних проблем, двояко пов'язаних з масштабністю технологічних ризиків і збільшенням швидкості та свободи доступу до інформаційних ресурсів для вирішення проблем комерційного, соціального, дипломатичного, військового характеру, інформаційної безпеки сучасних держав та ін.

Усвідомлення цього змушує визнати, що інформація і комунікації стають більш важливою складовою не тільки в контексті технологічного, а й державно-управлінського, соціального і культурного розвитку сучасної цивілізації.

Одночасно зростає переконання в тому, що ідеологічна і філософська інтерпретація процесів інформатизації, що розвивається в межах технологічного детермінізму, багато в чому звужує і формалізує рамки уявлень про дійсний характер, зміст і соціокультурний сенс процесів трансформації індустріального суспільства в постіндустріальний тип розвитку [357].

У цьому контексті дуже важливо звернути увагу на ту обставину, що розвиток інформаційно-обчислювальної техніки локалізує й спеціалізує в суспільстві нові види професійної зайнятості. Це пов'язано зі стрімким розвитком інформаційної діяльності як самостійного виду інтелектуальної

праці [130; 166]. До цього часу інформаційна діяльність розглядалася в прикладному аспекті, що значною мірою ускладнило інституційний розвиток інформаційного суспільства.

Не меншою проблемою залишається також розуміння характеру та особливостей впливу інформаційно-комунікаційних технологій на зміну традиційної системи діяльності людини. Особливо актуальним в сучасних умовах є виявлення ступеня впливу інформаційних чинників на систему безпеки сучасних держав. Це пов’язано з необхідністю пошуку підстав для розвитку інформаційної культури, що складає ядро розвитку сучасного типу соціальної культури та способу життя. Таке бачення основних проблем зміни зразків життєдіяльності та поведінки змушує висунути наукову гіпотезу про те, що положення людини в інформаційно-технічному світі визначено організаційно-психологічними змінами в характері соціального життя.

Можливості сучасної обчислювальної техніки та інформаційно-комунікаційних технологій зробили інформатизацію не тільки технічним феноменом, а й рушійною силою соціально-економічних і державно-управлінських змін сучасного суспільства. Інформатизація суспільства стає об’єктивним процесом, характер якого стимулює свідомий пошук нових критеріїв культури і соціального прогресу й активно впливає на зміни менталітету і способу життя людини, орієнтуючи індивідуальну та соціальну життєдіяльність людини на активну взаємодію з системами штучного інтелекту, що розвиваються [245].

Формування потреб у розвитку техніки в галузі державного управління, розвиток кібернетики та усвідомлення управлінських смислів, присутніх у природі інформаційних взаємодій, зробило інформацію найважливішим ресурсом соціально-економічного та державно-управлінського розвитку й породило зміни в загальній структурі системи діяльності сучасної людини. У зв’язку з цим стрімко зростає значущість і соціальна цінність інформаційної діяльності, яка стає однією з провідних

галузей сучасного виробництва й породжує інформацію як свій власний специфічний продукт.

Процеси розвитку інформаційної діяльності втягують сучасну людину в принципово нове коло культурних взаємодій і багато в чому впливають на усвідомлення людиною свого місця в соціальній культурі [350, с. 109].

В якості загальної основи соціокультурної і державно-управлінської динаміки розвитку життєдіяльності сучасної людини виступають об'єктивні процеси її інтелектуалізації та технологізації, які активно стимулюються компонентами технічного розвитку.

На нашу думку, ці процеси стають найважливішими факторами системотехнічної реструктуризації людської діяльності в постіндустріальну епоху. Вони створюють умови для розгляду класу інтелектуальних технологій як основи для перетворення організаційних форм різних видів діяльності в інформаційному суспільстві, обумовлюють професіоналізацію та спеціалізацію інформаційної діяльності, а також беруть участь в активному формуванні ринку інформаційних послуг.

Серед питань, які найбільш гостро стоять у зв'язку з розвитком інформаційних процесів і відносин, слід виділити проблему нерівномірності розвитку останніх у різних регіонах і країнах, що, у свою чергу, впливає на систему інформаційної безпеки держави.

Яка б не була економічна вигода від впровадження інформаційних і комунікаційних технологій, розподіл ІКТ-ресурсів (інформаційно-комунікативних) у світі носить вкрай нерівномірний характер. Існують значні відмінності не тільки між багатими і бідними країнами, а й між різними соціальними групами населення в кожній країні.

Наукові дослідження показали, що практично в усіх куточках світу доступ до можливостей інформаційного століття має лише певна частина населення. Як правило, не мають у своєму розпорядженні такої можливості малозабезпечені люди, яких особливо багато в країнах, що

розвиваються, і в країнах з перехідною економічною та державно-управлінською системами, до яких прийнято відносити пострадянські країни взагалі та Україну зокрема.

Серйозною проблемою є те, що ці відмінності не зменшуються, а повсюдно збільшуються. Це явище отримало назву «інформаційної» або «цифрової нерівності» (digital divide). Стурбованість появою нового виду соціальної диференціації змусила багато державних і громадських організацій всерйоз задуматися про плани подолання інформаційної нерівності.

З метою вирішення цієї проблеми ще у 2000 р. рішенням глав країн «Великої вісімки» була створена міжнародна цільова група «DOT Force». При цьому, як правило, розумілося, що під час обговорення інформаційних нерівностей малися на увазі, насамперед, різні можливості доступу до сучасних інформаційно-комунікаційних технологій і ресурсів. За цим критерієм можна зіставляти як різні країни світу, так і різні регіони, різні соціальні групи всередині країн [2, с. 41].

Дана проблема була визнана настільки важливою, що представники розвинених країн світу вважали за доцільне створити спеціальну робочу групу для підготовки рекомендацій главам держав G8 (з 2014 р. – G7) з розвитку інформаційно-комунікаційних технологій, розбудови глобальних мереж і принципів державного й міждержавного регулювання ІКТ-сектора.

Ці пропозиції потім були трансформовані в програму дій не тільки для країн-учасниць «Великої вісімки», а й в принципі для всіх держав-членів ООН, оскільки з самого початку головну роль у даній групі відігравали спеціалізовані організації, установи та представники ООН.

Згодом був розроблений план дій, що включав низку практичних рекомендацій за такими напрямками:

– підтримка розвиненими країнами розробки національних стратегій розвитку інформаційного суспільства (національних стратегій

електронного розвитку), що включають у себе в якості обов'язкового пункту створення електронних урядів;

– удосконалення, з урахуванням критерію вартості, інфраструктури доступу до інфокомунікаційних послуг;

– розробка цільових освітніх програм у сфері ІКТ для населення;

– широка міжнародна підтримка створення контенту національними мовами і локальних програмних додатків, адаптованих до особливостей тієї чи іншої країни, що розвивається;

– широке впровадження ІКТ у галузі освіти, охорони здоров'я, органи соціального обслуговування, громадянської активності.

Значущими в міжнародному досвіді виявилися ті основні групи заходів, які увійшли до програми дій, викладеної в рекомендаціях групи «DOT Force».

На першому місці стоїть вироблення національної стратегії електронного розвитку. Основні принципи реалізації даної програми в Україні викладені в концепціях національної та інформаційної безпеки України.

На другому місці – створення «людського капіталу», питання освіти, виховання, освіти. Далі – необхідність створення розвиненої інформаційно-комунікаційної інфраструктури. В успішному вирішенні цього завдання дуже велика роль держави і всієї системи державного управління в цілому.

Виконавча влада має досягти згоди в суспільстві, встановити пріоритети, сформувати середовище, яке сприятиме прискореному розвитку ІКТ, глобальних телекомунікаційних ліній зв'язку, становленню інформаційного суспільства.

І, нарешті, остання група рекомендацій з подолання інформаційної нерівності стосувалася створення нової економіки. На наш погляд, все вище сказане не втратило своєї актуальності і для України в сучасних

умовах (особливо у світлі минулих в Україні у 2019 р Президентських та Парламентських виборів).

Інформатизація має чіткий зв'язок з безпечним стійким розвитком суспільства і держави. Основа інформаційної економіки та державного управління – знання або інтелектуально-інформаційний ресурс. Знання мають незаперечні переваги в порівнянні з матеріальними ресурсами – фундаментом попередніх етапів розвитку суспільства [225].

Матеріальні ресурси жорстко підкоряються законам збереження. Якщо ви берете щось у природи – ви загострюєте екологічні проблеми, якщо ж намагаєтеся взяти у сусідніх країн – це породжує конфлікти і війни.

Соціально-економічна і державно-управлінська структура суспільства, що базується на інформаційній економіці та управлінні, вже за своєю суттю уникає більшості соціально-економічних проблем і в майбутньому передбачає розвиток суспільства за основними його параметрами («знання породжують знання»).

Особливість нової економіки і управління полягають в тому, що будь-яка людина у будь-якому куточку планети, отримуючи у свої руки останні технологічні досягнення, одночасно отримує й усі можливості для їх використання. У цьому – колосальна сила нових технологій: вони з таким же успіхом служать інструментом для створення добробуту в галузях промисловості, на сімейному рівні, на рівні освіти, в системі державного управління і т. ін.

Тобто йдеться про те, що інформаційні технології впливають на підвищення рівня життя кожної конкретної людини, сім'ї, поліпшення якості освіти, підвищення ефективності роботи системи управління державою як на місцевому, так і центральному рівні.

Глобальний характер інформаційного обміну та взаємодії робить актуальною цілу низку проблем інформаційної безпеки, що породжує у світового співтовариства потребу в створенні засобів і міжнародних

механізмів мінімізації небезпечних впливів на суспільство і державу внаслідок формування і руху інформаційних потоків [40, с. 103]. Таке завдання, безсумнівно, має вирішуватися на рівні ООН, Ради Європи, інших міжнародних організацій, найважливішою статутною метою яких є збереження мирного й безпечного розвитку світової спільноти.

Людство пов'язує свої надії на майбутнє з прогресом інформаційних технологій, розширенням і поглибленням сфери комунікацій. Інформатизація суспільства – не просто локальна сфера суспільного життя. Умови її розвитку лежать не тільки у сфері її технологій, інфраструктури, по суті вони охоплюють всі сфери життя суспільства, а їх наслідки глибоко зачіпають життя людини, суспільства, держави, і цей вплив все більше посилюється.

Зазначений вплив створює і в подальшому буде породжувати як позитивні, так і негативні наслідки, але поки вони усвідомлені, на нашу думку, далеко не повною мірою. Очевидним наслідком інформатизації суспільства є те, що людство неминуче робить величезний крок вперед на шляху формування «відкритого суспільства».

Глобальні інформаційні системи створюють безпрецедентні можливості поширення, запозичення, впровадження новітніх досягнень у різних сферах життя суспільства і прогресу в усіх регіонах і галузях. Водночас проникність сучасних носіїв інформації настільки велика, що всі заходи цілеспрямованого впливу на інформаційні потоки виявляються вкрай неефективними.

Тому вирішальним фактором у регулюванні процесів інформаційної взаємодії наразі залишається згода, консенсус міжнародних компетентних органів, учених, діячів культури, бізнесу, політики.

Сьогодні головне завдання полягає в тому, як зробити інформацію та канали її поширення більш надійними, засоби отримання – більш доступними, форми подачі інформації – культурно прийнятними, знання, цінності, що містяться в ній, – більш ефективними, корисними для людини

і суспільства. При цьому необхідно зберегти захищеними основні параметри функціонування держави, що є, на наш погляд, найважливішою складовою інформаційної безпеки держави.

Розвиток сфери інформації потребує всебічної міжнародної співпраці й передбачає створення сприятливого клімату взаємовідносин держав у політичній, економічній, культурній та державно-управлінській сферах життя суспільства.

Загальновизнано, що у своїй політиці світова спільнота повинна спиратися на загальні інтереси. Разом із тим і в сучасних умовах міжнародне співтовариство нерідко стикається з позицією домінування власних інтересів одних держав над інтересами інших, пріоритету силових методів вирішення проблем.

Безумовно, свій відбиток на прийняття рішень накладають рецидиви глибокі відмінності в рівнях розвитку країн, відсталості, агресивних устремлінь, тероризму, що ще зберігаються. Україна, як відомо, в результаті подій 2013–2014 рр. зіткнулась із серйозними загрозами своєї цілісності й втручання третіх країн у свої внутрішні справи.

У стратегічному плані перед світовою спільнотою постає питання, від вирішення якого залежить стабільність і просування до згоди з кардинальних проблем. У зв’язку з цим актуалізується питання співвідношення цінностей і принципів з національними інтересами. Як поєднати національні інтереси і глобальний стратегічний розвиток світової спільноти? Як, з одного боку, стати частиною глобального інформаційного простору, а з іншого – забезпечити інформаційну безпеку держави?

Оптимальний шлях – зосередити міжнародне співробітництво там, де воно приносить взаємовигідні плоди. Це, перш за все, координація в науково-технічних сферах: космічні дослідження, розробки в галузі ядерної фізики, створення нових матеріалів, екологічні програми. Сьогодні важко знайти сферу суспільного життя, де б в тій чи іншій формі не здійснювалося міжнародне співробітництво, кооперація зусиль у

досягненні певних цілей на рівні держав, громадських організацій, корпорацій, приватних осіб. І така співпраця може вийти на принципово нові кордони, буде значно заглиблюватися, якщо міжнародне співтовариство створить передумови сталого, інтенсивного розвитку систем інформації, кіберінформаційного простору.

Саме соціально-гуманітарні проблеми побудови стратегічних кіл в інформаційній сфері лягли в основу положень Окінавської хартії, прийнятої главами розвинених держав у 2000 р. [222]. Хартія цілком обґрунтовано ставить поруч проблеми інформатизації, побудови глобального інформаційного суспільства і боротьби з бідністю.

Подолання відсталості як у державно-регіональному, так і в соціально-груповому аспектах – це серйозна соціально-економічна і культурна проблема, ключова проблема світової політики. В аспекті інформатизації йдеться не тільки про те, що бідність обмежує доступність інформації й, отже, ще більше закріплює відсталість, поглиблює соціальні відмінності. Відсталість і неуцтво загрожують небезпекою для складно організованого технологічного співтовариства.

У вирішенні цієї проблеми не обійтися лише засобами військового та технічного захисту. Значно більші зусилля повинні бути спрямовані на забезпечення ефективної інформаційної безпеки держав. У сфері інформаційно-комунікаційних технологій йдеться, перш за все, про надання допомоги в розвитку інфраструктури, вдосконалення мережевого доступу, особливо у відсталих міських, сільських і віддалених районах, про більш легкий доступ в мережі для людей з меншою соціальною захищеністю, обмеженою працездатністю, що, на наш погляд, зокрема для України, є надзвичайно актуальною проблемою сьогодення [83].

Так, зокрема, це основне призначення реалізованої Європейським Союзом з початку 2000 рр. програми «Європейське інформаційне суспільство для зростання і зайнятості». А саме, з 1 червня 2005 р. в Європейському Союзі почалася реалізація програми «2010 – A European

Information Society for growth and employment» («Європейське інформаційне суспільство для зростання і зайнятості») – підвищення ефективності економіки шляхом використання ІКТ.

Програма базується на трьох основних принципах:

– створення єдиного європейського інформаційного простору, що сприяє розвитку відкритого конкурентного ринку ІКТ-технологій;

– зростання інвестицій у дослідження та інноваційні технології у сфері ІКТ;

– сприяння підвищенню якості державних послуг і якості життя в цілому шляхом використання ІКТ.

Слід зазначити, що програма побудована на вивченні досвіду найбільш успішних у сфері розвитку ІКТ країн, таких як Корея, Індія та Китай, де держава активно займається регулюванням ІКТ-галузі (або, як висловлюються автори програми, «веде здійснює індустріальну та інформаційну політику»).

Один із найважливіших принципів, проголошених в Окінавській хартії, – це доступність інформації. Сучасні інформаційні технології – це багаторазове множення для людини поля нових особистих контактів, знань, культурних досягнень. Проте цей новий світ інформації виявляється доступним лише для нової людини, підготовленої до взаємодії з подібним глобальним інформаційним простором, здатної орієнтуватися в ньому, проводити селекцію сприйняття інформаційних потоків, яка володіє імунітетом від негативних факторів впливу та інформаційних загроз. Підготовка виробника і користувача інформації, інформаційних систем та інформаційних послуг – це кардинальне завдання сучасної освіти.

Сучасна людина дедалі більшу частину дозвілля, свого емоційного життя, нині вже не тільки у сфері розваг, освіти, а й у сфері споживання, покупок, трудової зайнятості ось вже протягом десятиліть (покоління), пов’язує з технологічними електронними засобами інформації, що увійшли в побутовій вжиток.

Однак наскільки культура суспільства, психіка людини, сучасні структури спілкування, соціальні інститути адаптовані до умов «всепроникної інформації»? Де і як інформаційна експансія переходить ті межі, за якими йде руйнування особистості, культурних цінностей, втрачається керованість суспільного устрою? Де та межа, за якою вже пряма загроза існуванню держави, її інформаційної безпеки?

Загальний характер використання інформаційних технологій, глобальних мереж не знімає проблему відмінності інтересів між індивідами, соціальними групами, корпораціями, державами, міждержавними спільнотами як користувачами і виробниками інформації. Ці інтереси діючих в інформаційному полі суб'єктів включають тенденцію до зближення, розширюється сфера спільних інтересів, отже, в суспільстві посилюються інтеграційні процеси. Разом із тим зберігається проблема забезпечення самостійності, суверенності, захищеності в інформаційному просторі інтересів кожного суб'єкта, що діє: особи, держави, суспільства [186].

Як поєднати гуманітарні принципи права людини на інформацію, демократичні принципи відкритості інформаційного простору, гласності з інформаційною безпекою для громадських систем і людини?

Ця проблема гостро постала перед вченими, діячами культури, політиками, державними службами, громадськими організаціями. Проблема «інформаційної безпеки» з категорії вузько технологічної переходить у сферу концептуального обґрунтування управління суспільними процесами.

Параметри функціонування інформаційних систем від «оптимального» до «життєво небезпечного» стають все більш важливими індикаторами ефективності державного управління. Це складна проблема і вона багатогранна.

З інформаційним суспільством, що зараз формується, в останнє десятиліття пов'язуються великі очікування. Вважається, що воно має

величезний потенціал для поліпшення якості життя всього людського співтовариства і кожної людини окремо, різко розширює можливості для малого й середнього підприємництва, оптимального використання місцевих умов і ресурсів, розвитку управління, освіти та охорони здоров'я. На цій основі створюються передумови для значного підвищення ефективності існування сучасних держав у всіх сферах життя, в тому числі і в системі забезпечення інформаційної безпеки.

Разом з тим, усвідомлюючи всі переваги інформаційного суспільства, не можна не враховувати, що воно несе з собою не тільки нові рішення і можливості, а й нові проблеми та ризики.

Як і будь-яке інше, інформаційне суспільство недосконале, а ІКТ – нейтральні. Наслідки їх застосування залежать від ціннісних настанов і державно-політичних рішень. Реалізація можливостей інформаційного суспільства – питання адекватної політики і своєчасних державно-управлінських рішень.

На сучасному етапі розвитку, в умовах інтенсивного використання глобальних мереж виникають нові форми соціокультурної агресії з боку найбільш розвинених країн і регіонів щодо менш розвинених, з'являється небезпека втрати цілими спільнотами своєї культурної та національної ідентичності, включаючи мовну самобутність, відбувається нав'язування людству споживчих переваг і смаків в інтересах вузької групи транснаціональних компаній-виробників [210, с. 211].

Головна небезпека полягає в тому, що посилюється глобалізація виробництва, мобільність всесвітніх корпорацій, відбувається все більше проникнення інформаційних технологій у державно-управлінські процеси може несприятливо вплинути на безпеку держави.

В умовах існування відкритих, легкодоступних і таких, що постійно наповнюються інформаційних мереж, виникає проблема обмеження інформації, яка вважається соціально й економічно небезпечною, безпеки

персональних та інших видів даних, дотримання авторських прав і прав виробників електронної інформації.

Розвиток і широке використання ІКТ призвело до появи ще одного виміру бідності – так званої інформаційної. Це поняття відображає зростання соціальної диференціації населення за новим принципом – можливостей для користування сучасними ІКТ, коли лише частина населення отримує доступ до нових технологій та інформаційних ресурсів і може реалізувати цю перевагу.

Завдяки прискоренню процесу технологічних інновацій, залучення промислового капіталу і конкуренції нова мережева технологія та інфраструктура стають набагато дешевше, а тому доступніше все більшій кількості людей. Що стосується доступу до поширюваної різними новими каналами інформації, то це залишається однією з найскладніших проблем. Вартість інформаційних послуг може на багато років стати фактором, що підсилює розрив між тими, хто може, і хто не може собі дозволити отримувати й поширювати інформацію [353].

В останні роки ООН через реалізацію програми «Глобальні ініціативи щодо подолання інформаційної нерівності» дійшла висновку про те, що «соціальна та економічна нерівність, з якою ми стикаємося сьогодні, не тільки розширюється, але й стає все більш незбалансованою, тоді як чисельність бідних у світі продовжує зростати приголомшуючими темпами. Це чисельність збільшиться ще на два мільярди протягом наступних 50 років. З іншого боку, багатство сконцентровано в руках меншості, яка продовжує неймовірно процвітати від досягнень у сфері інформаційно-комунікаційних технологій. Сучасне суспільство має потребу, на наш погляд, у подоланні цієї нерівності шляхом співпраці та об’єднання зусиль державного та приватного сектора» [81].

Якщо говорити про більш віддалену перспективу, то тут справа може виявитися набагато складнішою. Йтиметься вже не про розрив між поколіннями в даному суспільстві, а про духовну, концептуальну,

культурну та діяльнісну прірву, яка відділяє інформаційно-насичені цивілізації від країн і народів, що пішли не шляхом науково-технологічного прогресу, а шляхом культурної, цивілізаційної та концептуальної самоізоляції, утвердження свого «особливого», неповторного, наперед визначеного етнокультурного шляху, який може привести тільки до незворотної відсталості [354].

В сучасних умовах, на наш погляд, можна говорити про сформовану і продовжує розвиватися конфедерації європейських країн, що мають глибокі історичні, моральні, релігійно-філософські та світоглядні корені, але це не означає деіндивідуалізацію й повну аккультурацію [335].

Насправді йдеться про перехід цілої групи європейських культур, разом із культурою США, Японії і деяких інших азіатських країн, на новий щабель історичного розвитку, де їх своєрідність не зникне, а можливо навіть збережеться й посилиться, але на зовсім іншій платформі – на платформі інформаційної цивілізації [318; 361].

У цьому сенсі шлях, який обрала Україна як держава, лежить, на наш погляд, саме в цій площині.

Вирішення розглянутих у даному підрозділі проблем становлення інформаційного суспільства в контексті проблем, пов’язаних із забезпеченням та захистом інформаційних комунікацій Української держави, вимагає серйозних зусиль фахівців різних сфер.

При цьому необхідно враховувати, що методи протидії всім перерахованим та іншим небезпекам інформаційного століття лежать не у сфері відгородження країни або окремих груп від глобального інформаційного суспільства, а у сфері розвитку повноцінної участі в його формуванні.

Оцінюючи результати перспектив забезпечення інформаційної безпеки в умовах становлення глобального інформаційного суспільства, можна зробити такі висновки.

1. Для сучасного етапу розвитку інформаційного суспільства є характерною нерівномірність розвитку й розподілу інформаційно-комунікаційних технологій у різних державах і куточках світу, що отримало офіційну назву «цифровий розрив», або «інформаційна нерівність». Зараз у цьому плані спостерігаються суттєві відмінності не лише між розвиненими країнами та країнами, що розвиваються, а й між різними верствами населення всередині кожної держави.

2. У міру формування інформаційного суспільства розвивається і глобальна система інформаційної безпеки. Умовою еволюційного, поступального переходу України на новий етап розвитку є перетворення її національних інтересів на природну, обов'язкову складову інтересів глобального інформаційного співтовариства, тоді її інформаційна безпека також стане одним із елементів глобальної системи такої безпеки.

3. Інформаційне суспільство породжує не лише нові можливості, а й нові загрози і ризики. Як і всі інші суспільства, інформаційне теж не є досконалим, а ІКТ самі по собі є нейтральними – наслідки їх впровадження зумовлюються ціннісними установками і політичними рішеннями держави. Умовами успішної реалізації позитивних можливостей такого суспільства стають загальна адекватність політики та своєчасність ухвалення державно-управлінських рішень.

2.2. Комунікація державного управління та суспільства як чинник формування та реалізації політики інформаційної безпеки держави

Сучасна інформаційна революція у світі диктує нову інформаційну парадигму у вивченні політичних і державно-управлінських явищ. Як ми вже зазначали в попередньому підрозділі, під впливом інформаційних технологій змінюються і державно-управлінські інститути, політичні

відносини, форми політичного й управлінського впливу на суспільство і суспільну свідомість та способи пізнання політичних реалій.

Унаслідок цих змін державне управління інформаційними потоками й інформаційними технологіями стає головним важелем державної влади, а процеси управління інформаційними потоками визначають успіх майбутнього державного розвитку.

Слід наголосити, що в рамках комунікативного підходу державна влада інтерпретується як обмежена в часі і просторі субстанція впливу, підпорядкування, сили або відносин.

На нашу думку, це особливий різновид соціальної взаємодії державно-управлінських суб'єктів, специфічна форма соціальної комунікації між суб'єктами і об'єктами державно-управлінської діяльності з приводу отримання, зберігання, відтворення і трансформації державно-управлінської інформації з метою вироблення адекватних або неадекватних політичних цінностей суспільства рішень [271, с. 54].

У цьому контексті в дослідженні природи державно-політичної влади насамперед слід виділити онтологічну концепцію відомої дослідниці Х. Арендт. На її думку, розуміння комунікативності соціальної і державно-управлінської реальності та її політичної складової можливо лише в рамках онтологічно-інституціонального підходу, оскільки лише такий підхід у змозі розкрити основоположні, сутнісні сторони й аспекти світу політичної влади [307].

Очевидно, що саме до таких інституціональних структур належить державна влада. Загалом вона й державне управління зокрема – це «інституціоналізація впливу і ціннісної системи», а державна влада – і складний фактор детермінації соціальних подій, і форма державно-управлінської інституціоналізації, до якої входять легітимація і керівництво.

На думку відомого вченого Т. Парсонса, політична влада – це не тільки здатність конструювати рішення, засновані на колективності, а й

такий спосіб соціальної дії індивідів, який обов'язково обумовлюється наявністю публічного інтересу. Тільки в цьому випадку про владу можна говорити як про гранично загальний політичний інститут [цит. за 236, с. 176].

Теоретичними джерелами розробки інформаційно-комунікативних аспектів діяльності владних структур, безсумнівно, є також концептуальні уявлення Н. Лумана про комунікативну природу влади і влади як засобу комунікації, Ю. Хабермаса про роль комунікативної компетентності, про розвиток комунікативного розуму [348; 349].

Серед праць, присвячених даній проблематиці, можна виділити ті, що засновані на аналізі теорії соціального психоаналізу, взаємодії свідомого, підсвідомого й несвідомого при впливі на них сенсорної і субсенсорної інформації; враховуючи закон «ментальної ідентичності» в інформаційній політиці, в них обґрунтовується єдність економічних, політичних, духовних, творчих і соціо-комунікативних критеріїв в оцінці інформаційного менеджменту [360].

Комунікативна підсистема державно-управлінської системи суспільства – це сукупність відносин і форм взаємодії, що складаються між класами, соціальними групами, націями, індивідами з приводу їх участі в здійсненні влади, виробленні та проведенні політики.

Узагалі, політичні та державно-управлінські відносини є результатом численних і різноманітних зв'язків суб'єктів політики в процесі політичної діяльності. Вступати в них людей спонукають їх власні політичні інтереси і потреби.

Виділяють первинні і вторинні (похідні) політичні відносини. До перших відносяться різні форми взаємодії між соціальними групами (класами, націями, станами та ін.), а також всередині них; до других – відносини між державами, партіями, іншими політичними інститутами, що відображають у своїй діяльності інтереси певних соціальних верств або всього суспільства [155; 233].

Особливим аспектом комунікативної підсистеми соціуму є відносини між державно-управлінськими структурами і суспільством. У сучасних умовах цей аспект все частіше стає предметом наукових досліджень.

На нашу думку, необхідно враховувати особливу значущість того факту, що об'єктом національної безпеки в інформаційній сфері виступають інформаційні права і свободи громадян, а також те, що безпека являє собою явище суспільно-політичне.

Виходячи з цього, стає очевидним, що в умовах відданості демократичним принципам ключовим моментом забезпечення безпеки суспільства і держави повинна стати опора саме на цінності і пріоритети громадянського суспільства, на основі співробітництва і ідеї взаємовигідного партнерства.

У цьому контексті, як нам уявляється, набуває актуальності проблема якісних змін у діяльності органів державної влади та всієї системи управління, перетворення системи державного управління з урахуванням вироблення механізму узгодження інтересів керованих і керуючих, які повинні отримати підставу в законодавстві, у громадській свідомості й політичній культурі державних службовців, політиків і громадян.

З ефективністю інформаційно-комунікативної взаємодії влади і суспільства, з підвищенням відкритості та доступності пов'язана проблема довіри громадян до інститутів публічної влади. Як засвідчують дані соціологічних досліджень, проведених останнім часом різними центрами дослідження громадської думки, громадяни України досить критично ставляться до більшості інститутів влади і державного управління.

Так, на думку експертів Київського міжнародного інституту соціології (КМІС), у кінці 2018 р. найменшою довірою громадян України користувалися Президент (16 %), Уряд (11 %), Верховна Рада (8 %) і російські ЗМІ (4 %). КМІС провів проводив опитування з 30 листопада по 14 грудня 2018 р. серед 2034 респондентів по всій Україні, за винятком окупованих Росією територій. Статистична похибка вибірки (з імовірністю

0.95 і з дизайн-ефектом 1.5) не перевищує: 3,3 % для показників, близьких до 50 %; 2,8 % – для показників, близьких до 25 %; 2,0 % – для показників, близьких до 10 %; 1,4 % – для показників, близьких до 5 % (рис. 2.1).

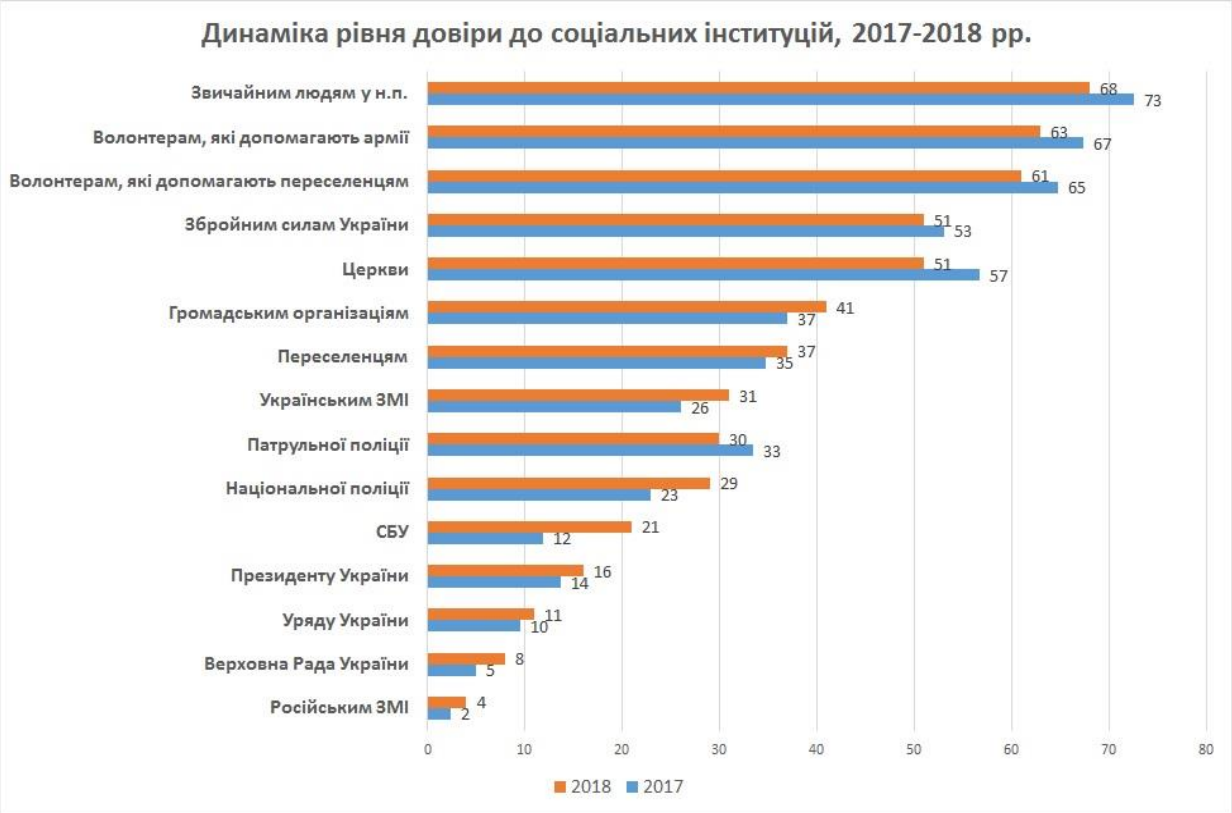

Рис. 2.1. Динаміка довіри громадян України до соціальних інституцій протягом 2017–2018 років

Джерело: складено на підставі статистичних даних kiis.com.ua

Україна посіла перше місце за рівнем недовіри до влади. Такі показники країна показує вже другий рік поспіль. Так, владі в Україні довіряють лише 9 % населення. Такі дані дослідження оприлюднила аналітично-консультативна компанія Gallup за 2018 р. [86].

У сучасних умовах, на нашу думку, внаслідок протиріч влади і суспільства комунікативна діяльність органів влади характеризується такими ознаками, як недостатня відкритість, фрагментарність, маніпулятивність технік. Це підтверджується урядовими стратегіями інформування, тактиками комунікативної поведінки представників влади,

соціальними практиками професійних PR-агентств, які виконують державні замовлення.

У зв'язку з цим, на нашу думку, недостатня соціальна відповідальність влади й особливості її комунікації детерміновані інструментальним підходом. Публічні служби використовуються як інструмент збереження владних інтересів, конструювання одностороннього бачення смислів державно-управлінських рішень. В цілому комунікативна модель формування та підтримки відносин з суспільством характеризується як одностороння, в результаті чого утворюється розрив між реальною політикою і інформаційним продуктом, що створює негативні наслідки для легітимності влади.

Сьогодні дуже актуальна проблематика, пов'язана з вивченням потенціалу і місця інформаційно-комунікативних технологій (ІКТ) в системі державного управління та політики в цілому. Ці проблеми стали об'єктом уваги дослідників ще в 60-х роках XX ст., але реальні можливості по втіленню існуючих концепцій в життя з'явилися тільки на початку 1990-х рр.

Завдяки науково-технічному прогресу з'явилися нові технології обробки, передачі й зберігання інформації, засоби електронної політичної та державно-управлінської комунікації, причому темпи їх впровадження в державно-управлінську сферу життєдіяльності суспільства останнім часом різко зростають. Досить поглянути на систему інформаційного забезпечення органів влади України в останні роки і можна переконатися в тому, що інформаційні технології активно використовуються в державному управлінні. Особливо явним це стало з приходом до влади в Україні у 2019 р. нової державно-управлінської «команди». Вони застосовуються в процесі прийняття політичних і державно-управлінських рішень як інструмент впливу громадянського суспільства та оптимізації владних відносин. Все це сприяє перетворенню інформаційно-

комунікаційних технологій на важливий фактор державно-політичного процесу.

На думку ряду фахівців у сфері масових комунікацій (І. Додін, Р. Почепцов, С. Чукут та ін.), затребуваність вивчення політико-управлінських аспектів використання ІКТ в системі державної влади обумовлюється їх великим творчим потенціалом у вирішенні управлінських проблем і перспективністю інформатизації суспільства [100; 125].

Одним із результатів широкого використання ІКТ у діяльності державно-управлінських структур повинна стати, на наш погляд, реалізація концепції інформаційної безпеки України. Особливо це стосується питань створення «електронного уряду», а також в частині усунення недоліків в реалізації державної інформаційної політики.

Важливість створення електронного уряду, усунення серйозних прорахунків у формуванні ефективної системи інформаційної безпеки в ході формування в Україні інформаційного суспільства неодноразово відзначалося на всіх рівнях державної влади.

Як наголошується в доктрині інформаційної безпеки України, «недостатня розвиненість національної інформаційної інфраструктури не дає можливості Україні ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України». В доктрині підкреслюється «неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства» [248].

Широке використання ІКТ в системі центральних і регіональних органів державної влади є сьогодні нагальним завданням. Насамперед це зумовлюється необхідністю оптимізації державного управління на всіх

рівнях влади, забезпечення його прозорості й доступності для громадян, результативної взаємодії з інститутами громадянського суспільства

За допомогою ІКТ громадяни отримують реальний шанс брати участь у діалозі з владою, впливати на прийняття управлінських рішень та висувати власні ініціативи, отримувати детальну інформацію про роботу державних структур і здійснювати контроль за їх діяльністю тощо.

Сприяти суттєвому просуванню у справі інформатизації державного управління покликана децентралізація державної влади та управління, яка реалізується в Україні й розрахована (Стратегія сталого розвитку «Україна – 2020») на період до 2020 р. [249]. При цьому слід зазначити, що з приходом до влади в Україні у 2019 р. нової політико-управлінської «команди», необхідність проведення такої реформи, як і більш глибока модернізація інформаційної сфери, як і раніше надзвичайно актуальна. Основною метою програми є використання ІКТ для підвищення ефективності функціонування державного і місцевого управління. Однак, як показує практика, для їх успішної реалізації необхідно подолати низку перешкод.

Так, зокрема, на відміну від країн Європи, де створення «електронного уряду» є частиною адміністративної реформи, в Україні реформа децентралізації державного управління та здійснення програми «електронного уряду» йдуть паралельно, що заважає чіткої координації між ними [1].

Застосування нових інформаційно-комунікаційних технологій в державному секторі поки здійснюється значною мірою в інтересах забезпечення діяльності самих державних структур (побудова інформаційних систем, баз даних, локальних і корпоративних мереж, впровадження електронного документообігу і т. ін.) [241].

Наприклад, сьогодні багато як державних, так і бізнес-структур створюють потужні інформаційні системи – ситуаційні центри, інформаційно-аналітичні центри і т. ін. Їх поява часто носить не зовсім, на

наш погляд, системний характер, а десь і просто є віянням моди. Досить часто не визначено цілі, завдання, механізми та архітектура системи управління, в інтересах якої вони повинні працювати. Крім того, завантаженість й ефективне використання таких інформаційних систем зводиться до мінімуму через те, що функціонують вони значною мірою в автономному режимі.

У питаннях міжвідомчої взаємодії, як правило, відсутні взаємопов'язані інформаційні завдання та технології підтримки прийняття рішень, що не дозволяють об'єднати такі інформаційні системи в єдину мережу.

Такі ж проблеми мають місце і на регіональному рівні. Як наслідок, управлінські рішення приймаються в обхід створених інформаційних систем, що стоять адміністративно й організаційно-технологічно відособлено, осторонь, на основі наявної і не завжди повної інформації, а взаємодія втрачає повноту й оперативність [143].

У розвинених країнах в останнє десятиліття ведуться роботи зі створення електронних урядів, що будуються на принципах відкритості, «одного вікна» і зворотного зв'язку. Наприклад, свої національні програми переходу до інформаційного суспільства розробили і реалізують Великобританія – «UK online», США – «Національна інформаційна інфраструктура», Франція – «Government Action Program for Information Society» та інші країни, а також Євросоюз – «eEurope» [154].

Розвиток цих програм знаходить своє відображення в законодавчих актах цих країн. За право брати участь в створенні електронних урядів в різних країнах сьогодні «б'ються» найбільші світові виробники інформаційно-комунікаційних технологій – Microsoft, IBM, Hewlett-Packard, Cisco Systems та ін. [337].

Лідерство у формуванні національного інформаційного суспільства належить США. Влада цієї країни виділяє величезні фінансові кошти на розвиток інформаційно-комунікаційних технологій, тому що бачать у них

потужний стимул для своєї економіки та системи управління. Головний урядовий портал США – FirstGov – об'єднує в собі близько 30 млн урядових Web-сторінок задля забезпечення більш ефективного пошуку необхідної інформації та надання державних послуг громадянам країни. Уже сьогодні близько 20 % всіх податків і штрафів в Америці збираються через Інтернет [221; 337].

Однак у США існує низка проблем як у державному, так і приватному секторах: має місце відставання в темпах інформатизації державних органів, а також не всі американські сім'ї здатні придбати персональні комп'ютери [337].

У цьому плані ситуація в Україні виглядає ще гірше. У суспільстві ще досить сильно недовіру до впровадження нових технологій в процес державного управління Так, 81 % американців стурбовані можливістю втрати своїх персональних даних на урядових сайтах, 63 % не бажають надавати свою персональну інформацію, а 72 % побоюються використовувати електронний цифровий підпис. Багато проблем, в тому числі й зазначені вище, є загальними для країн, залучених до процесу розвитку інформаційного суспільства. Проблеми захисту персональних даних надзвичайно актуальна і для України.

Як показує вітчизняна практика створення «електронного уряду», сьогодні спостерігається значний перекіс у бік надання інформаційних послуг (довідкова інформація, стрічки новин та ін.), Менша увага приділяється механізмам активного спілкування з громадянами та надання їм затребуваних інтерактивних послуг. Створені в Інтернеті офіційні сайти органів державної влади часто мають недостатнє інформаційне наповнення і не підтримують надання державних послуг.

Проблеми формування та розвитку державних інформаційних систем загального користування є сьогодні, на наш погляд, надзвичайно актуальною проблематикою щодо інформатизації суспільства і

вибудовуванні ефективної комунікації між громадянами та системою державного управління.

Моніторинг офіційних сайтів органів державної влади України свідчить про те, що рейтинг їх відкритості, під якою розуміється готовність надавати інформацію та державні послуги громадянам за допомогою українського сегмента Інтернету, відносно невисокий.

При складанні рейтингу необхідно, на нашу думку, використовувати спеціально розроблену методику і враховувати такі критерії оцінки, як наявність або відсутність інформації, її повнота, доступність і актуальність. Можна відзначити, що в останні роки намітилася позитивна динаміка якісних і кількісних характеристик інформації, розміщеної на офіційних сайтах органів державної влади України. Разом із тим слід зазначити, що якість сайтів далеко не завжди відповідає вимогам сьогодення й більшість з них не відповідають:

– нормам законодавства, що регулює доступ до інформації про діяльність державних органів;

– загальноприйнятим технічним вимогам, що пред'являються до змісту сайтів;

– потребам фізичних і юридичних осіб в інформації з державних інформаційних ресурсів.

Все це свідчить про те, що існує реальна потреба в науковому вивченні можливостей і напрямків використання інформаційно-комунікаційних технологій у системі державного управління.

Слід зазначити, що питання, пов'язані з електронним урядом, активно досліджуються сьогодні в наукових колах [5; 65; 66; 232; 261], багато авторів розглядають його як електронну інфраструктуру інститутів публічної влади, доповнену системою інтерактивної взаємодії держави і громадян за допомогою Інтернету. Більшість авторів сходяться на думці, що це нова модель державного управління, яка перетворює традиційні відносини громадян і владних структур.

Зв’язок процесів формування електронного уряду та процесів децентралізації розкривається в роботах багатьох дослідників [65; 232]. Відповідно до їх підходу, електронний уряд розглядається, головним чином, з точки зору оптимізації та підвищення ефективності взаємодії органів влади. Відзначається, що його впровадження має низку позитивних аспектів для самої влади.

Так, електронне урядування дозволяє легше здійснювати моніторинг дієвості та ефективності уряду в сфері надання послуг, спрощує і робить прозорим фінансовий менеджмент, управління персоналом, програмами, змінами і т. ін.

Виходячи з того, що електронний уряд – це концепція здійснення державного управління, притаманна інформаційному суспільству, багатьма авторами були розглянуті принципи його організації, основні критерії та цілі. У цьому контексті слід виділити роботи І. Додіна, Г. Почепцова, С. Чукут, В. Степанова [100; 237; 265; 266] та низки інших авторів, які досить детально розглядали механізми впровадження ІКТ в систему органів державної влади, інформаційно-комунікативні форми її організації, проблеми реалізації концепції «електронного уряду», нормативно-правову базу та програмні заходи процесу інформатизації.

На нашу думку, слід звернути увагу і проаналізувати новації, пов’язані з прийняттям Закону України «Про доступ до публічної інформації» [240]. Даний закон, прийнятий у 2011 р. і більшою мірою адаптований до сучасних життєвих реалій і телекомунікаційних процесів, які зазнали значних еволюційних змін за час, що минув після прийняття Закону України «Про інформацію» (1992 р.) [242].

Однак, попри це, істотною проблемою залишається відсутність чітких механізмів, важелів, завдяки яким цей закон регулював би суспільні відносини. Цими механізмами повинні були бути підзаконні нормативні акти або інші закони, що чітко регламентують дію всіх процесів,

пов’язаних з інформацією, інформаційними технологіями та захистом інформації.

Про незадовільний стан державної системи підтримки інформаційних ресурсів свідчить та обставина, що ця система не стандартизована й має розриви між регіональним та центральним рівнями.

У більшості випадків комунікація між базами даних різних відомств і служб опосередковується «паперовими» запитами, що пересилаються звичайною поштою. В цілому український державний сегмент Інтернет-ресурсів значно відстає від комерційного в реалізації потенціалу та використанні технологічної потужності й інтерактивних можливостей середовища Інтернет для забезпечення ефективної взаємодії органів влади з населенням країни [356].

Слід зазначити, що правове поле інформаційних відносин на території України як на регіональному, так і на центральному рівні, вкрай невпорядкований. Так, всі існуючі бази даних в органах державної влади мають довідковий характер і не є юридично значущими, що не дозволяє використовувати дані з них, наприклад, під час розгляду судових суперечок [128].

На регіональному рівні відчувається дуже низький концептуальний, нормативно-правовий, організаційний та технічний рівень забезпечення сайтів більшості регіональних органів державної влади. Це проявляється в тому, що, як правило, для користувачів Інтернету немає єдиної точки доступу до інтернет-ресурсів українських органів державної влади, відсутній єдиний механізм пошуку і навігації за всіма доступними ресурсами. Крім того, не створено систему надання інформації за основними напрямками діяльності органів влади, що пояснюється відсутністю коштів і необхідної кваліфікації фахівців, відповідальних за підтримку відповідних державних Інтернет-ресурсів.

Відсутні також загальні для всіх органів державної влади організаційні, нормативно-правові та технічні стандарти у сфері надання

органами державної влади інформації та послуг через Інтернет, не створено системи взаємодії і взаємозв'язків окремих державних Інтернет-ресурсів між собою.

Узагальнюючи думки експертів, сформулюємо основні причини низького рівня реалізації можливостей інформаційно-комунікаційних технологій як в регіонах, так і в країні в цілому.

1. Відсутня єдина інфраструктура зв'язку та інформації державних органів влади, побудована на єдиних стандартах і платформах, що ускладнює процес своєчасного впровадження сучасних технологій. Діючі інформаційні системи органів державної влади були розроблені і введені в експлуатацію в різний час, що сьогодні зумовило несумісність програмно-технічних рішень.

2. Спостерігається суттєве відставання України від провідних країн у розвитку інформаційно-комунікаційної інфраструктури, виробництва інформаційних і комунікаційних засобів, продуктів і послуг.

3. Має місце недостатність державних ресурсів для розвитку інформаційно-комунікаційної інфраструктури як на центральному, так і регіональному рівні.

4. Існує обмеження попиту на сучасні послуги зв'язку, в тому числі послуг мережі Інтернет значною частиною населення з низьким рівнем життя. Особливо це стосується сіл, селищ і невеликих міст.

5. Констатується неготовність більшої частини населення до умов життя в інформаційному суспільстві. Широко поширена комп'ютерна неграмотність, нерозвинена мотивація використання сучасних технологій, як наслідок – відсутні знання про можливості використання інформації.

У цих умовах передчасно говорити про використання будь-якої ефективної технології зворотного зв'язку.

Для просування вперед в напрямку підвищення ефективності інформаційно-комунікативної діяльності органів державної влади необхідно вжити низку заходів, серед яких, на наш погляд, повинні бути:

– розробка положення про типову структуру інформаційної системи органів державної влади різних рівнів, в якій визначався б перелік обов'язкових інформаційних підсистем (наприклад, електронний документообіг, електронний цифровий підпис, захист інформації, електронна комерція, електронний архів, доступ до Інтернету і т. ін.);

– перелік обов'язкових актуальних інформаційних ресурсів (які формуються, надаються, доступні й т. ін.).

Це надасть можливість виробити критерії об'єктивного оцінювання рівня інформатизації органів влади. У свою чергу результати такої оцінки дозволять визначити заходи щодо усунення інформаційної нерівності між регіонами України, відповідно розподіляючи обсяги фінансування інформатизації.

Самі по собі інформаційно-комунікаційні технології, як ми вже неодноразово вказували, політично нейтральні: вони можуть використовуватися як в тоталітарній, так і в демократичній державі. Для гарантій дотримання інтересів громадян і захисту демократичних цінностей при використанні інформаційно-комунікаційних технологій слід актуалізувати певну систему принципів, законодавчих та організаційних заходів [138]. У зв'язку з цим, на наш погляд, розглянуті проблеми слід аналізувати в контексті інформаційної безпеки особи, суспільства і держави.

Підбиваючи підсумки, можна дійти таких висновків.

1. Особливий аспект комунікативної підсистеми соціуму становлять відносини між владними структурами та суспільством.

2. У сучасній Україні комунікативна модель формування та підтримки відносин держави з суспільством характеризується як одностороння. Зворотній зв'язок із суспільством є досить слабким.

3. У сфері формування електронного уряду існує явний перекіс у бік надання інформаційних послуг, часто незатребуваних суспільством.

4. Неможливість суспільства частково або повністю реалізувати свої конституційні права в інформаційній сфері негативно впливає на стан інформаційної безпеки Української держави і соціуму в цілому.

5. Спостерігається пряма залежність: чим гіршим є взаємозв'язок суспільства і держави, тим нижчим буде рівень інформаційної безпеки України, і навпаки. У цьому випадку відбувається спонтанне формування невзаємопов'язаних локальних політик інформаційної безпеки громадян, суспільства і держави, що призводить до зниження ефективності інформаційної безпеки України.

2.3. Інформаційна безпека в державно-управлінських відносинах в контексті процесів демократизації суспільства

Розвиток сучасних держав, як уже зазначалось у попередніх підрозділах, характеризується двома провідними тенденціями: глобалізацією та інформатизацією, базовою основою яких виступають інформаційні технології [314, с. 22]. У зв'язку з цим інформація, на нашу думку, має пряме відношення до державно-управлінських відносин у сучасному світі.

Результати розвитку інформаційних технологій дозволяють висунути наукову гіпотезу про те, що в найближчому майбутньому буде створено більш динамічну, ніж сьогодні, світову інформаційну модель. В останні роки неймовірно зростала інтенсивність споживання інформації в усіх сферах життєдіяльності людини і суспільства – соціальній, науково-технічній, технологічній, державно-управлінській, економічній та ін.

Процеси збору, накопичення, переробки та поширення інформації стають необхідною умовою ефективного функціонування існуючих структур державного управління, здійснення державно-політичних впливів на все суспільство, вирішення масштабних економічних завдань. При цьому слід мати на увазі, що інформація – це не тільки сила творити. На

жаль, вона володіє дестабілізуючими факторами, які можуть впливати на суспільство і систему державного управління.

Можна припустити, що в сучасних умовах використання інформаційних ресурсів створює практично необмежені можливості впливу на людину, суспільство та державне управління і далеко не завжди це відбувається в інтересах суспільства і держави.

Досвід останніх десятиліть розвитку сучасної людської цивілізації засвідчив очевидне: інформація може стати джерелом політичної та соціальної загроз, що зумовило необхідність державно-управлінського та громадського регулювання інформаційних потоків.

На наш погляд інформаційне суспільство в політико-управлінському відношенні має являти собою демократію з широкими можливостями впливу громадян на владу, їх участі у формуванні та здійсненні всіх функцій держави.

Як уже зазначалось у попередньому підрозділі, такі можливості багато в чому можуть реалізовуватися завдяки новій технологічній базі («електронний уряд»). Однак, на нашу думку, в найближчі роки ефективність інформаційної безпеки держави все більше буде визначатися помітно зростаючим впливом електронних засобів масової інформації та Інтернету, які відіграють все більшу роль як у політичному житті, так і в системі управління державою.

Сьогодні державні структури, політичні партії, громадські об’єднання відкривають свої сайти і портали. Потенційно вище стають можливості громадян брати участь у політично творчому процесі – обговоренні законопроектів, висуненні ініціатив, у процесі соціальних інновацій, сигналізувати державі про проблеми, що виникають у різних сферах сучасного суспільства.

Сьогодні стало практично правилом, коли державні структури і багато державних управлінців комунікують із суспільством за допомогою

мережевої структури суспільства. Соціальні мережі нині виступають впливовим фактором як для отримання інформації, так і для формування суспільної свідомості.

У зв'язку з інтенсивною інформатизацією державно-управлінських відносин, політичного процесу вельми актуальною стає проблема забезпечення інформаційної безпеки в цій сфері.

Концепція інформаційної безпеки України визначає основні категорії і поняття в даній сфері державної політики. Зокрема, під інформаційною безпекою розуміється стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, який дозволяє запобігти завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [69; 70].

У зв'язку з цим, на наш погляд, абсолютно очевидним є той факт, що інформаційна безпека у сфері державно-управлінських відносин у політичному процесі може розглядатись як сукупність взаємодіючих і взаємопов'язаних компонентів, а саме:

– загрози життєво важливим інтересам суспільства у сфері інформаційної безпеки, а також небезпеки, виклики та ризики;

– самі життєво важливі інтереси суспільства, держави та особи, що підлягають інформаційному захисті;

– основні заходи, що проводяться суб'єктами держави і громадянського суспільства, з нейтралізації загроз, небезпек і ризиків у сфері інформаційної безпеки [322].

З процесуальної точки зору інформаційна безпека в державно-управлінських відносинах може бути представлена такими основними напрямками:

– інформаційна безпека сфері державно-політичних інтересів;

– інформаційна безпека в системі державного управління;

– інформаційна безпека в процесі партійного будівництва;

– інформаційна безпека зовнішньополітичного процесу і т. п.

За основними сферами прояву системне вираження інформаційної безпеки локалізується в трьох напрямках:

1. Інформаційна безпека у сфері функціонування державних органів політичної влади (державна інформаційна безпека).

2. Інформаційна безпека, здійснювана у сфері громадянського суспільства (громадська інформаційна безпека).

3. Інформаційна безпека особи, а також особиста інформаційна безпека.

Нарешті, за рівнями соціальної організації й геополітичним змістом інформаційна безпека виступає у вигляді таких компонентів:

– інформаційна безпека, яку забезпечують на міждержавному рівні;

– інформаційна безпека на національно державному рівні;

– інформаційна безпека окремих регіонів на внутрішньодержавному рівні;

– інформаційна безпека, яку забезпечують на рівні органів місцевого самоврядування.

Оскільки державно-управлінський процес в умовах соціальної трансформації багатий і різноманітний, то всі без винятку його основні компоненти виступають об’єктом докладання інформаційної безпеки.

Таким чином, в інформаційному суспільстві інформаційна безпека являє собою багаторівневу систему, що включає інформаційну безпеку індивіда, суспільства і держави, які взаємопов’язані між собою. При цьому інформаційна безпека даних об’єктів багато в чому залежить від інформаційної безпеки таких ключових інститутів державно-політичної системи, як система масових електронних комунікацій.

При аналізі інформаційної безпеки державно-політичного процесу в Україні в умовах її соціальної і державно-політичної трансформації слід враховувати своєрідність її параметрів і пріоритетних компонентів.

По-перше, в період трансформації система інформаційної безпеки відчуває етап свого становлення з усіма його складнощами і невизначеностями.

По-друге, в силу того, що для процесів державного управління пріоритетними й актуальними компонентами системи інформаційної безпеки виступають такі, що безпосередньо пов'язані з інститутами демократизації і громадянського суспільства, багатопартійністю і виборною системою, які є, на наш погляд, недостатньо розвиненими в Україні.

По-третє, остаточне формування параметрів і компонентів системи інформаційної безпеки в Україні буде залежати від успішної нейтралізації інформаційних загроз, небезпек і ризиків, характерних для періоду соціальної та державно-політичної трансформації.

У теоретичному плані розгляд проблем інформаційної безпеки державно-управлінської сфери тісно пов'язаний з проблемою співвідношення інформатизації суспільства з процесами його демократизації.

У пострадянської політичної та державно-управлінської науки з кінця 1990-х рр. досить широко поширеною є точка зору, згідно з якою інформатизація і демократизація знаходяться в діалектичних взаємовідносинах. З одного боку, інформатизація несумісна з тоталітарним режимом, тільки демократизація суспільного життя створює для неї сприятливі умови. Таким чином, можна сформулювати наукову гіпотезу про те, що інформатизація суспільства вимагає її демократизації. З іншого боку, інформатизація в сучасних умовах є потужним засобом розвитку

демократичного устрою, позбавлення від бюрократичної сваволі, стимулом розвитку політичної та економічної активності громадян [343].

Розвиток демократії створює сприятливий соціальний клімат для інформатизації. Інформатизацію, згідно з даної точки зору, можна назвати супутником сучасної демократії, вона неможлива без подальшої демократизації.

Інформатизація суспільства, що розуміється як розвиток за допомогою інформаційних засобів пізнавальних соціальних структур і процесів, повинна знаходитися в органічній єдності з процесами соціальної інтелектуалізації, істотним підвищенням творчого потенціалу особистості [212].

Іншими словами, взаємини демократії та інформатизації полягають в тому, що інформатизація, будучи залежна від певних соціально-політичних, економічних і державно-управлінських умов, у свою чергу здійснює як би зворотний вплив на ці умови, в тому числі на процеси демократизації.

Оскільки демократія є важливим елементом політичного життя, а політика і система державного управління – це форми комунікації, неможливі без політичної організації, націленої на оволодіння владою, то сили, що прийшли до влади, формують комунікації відповідно до своїх інтересів і потреб [345]. Формування комунікації ґрунтується на використанні комунікаційних засобів, серед яких інформатика в сучасних умовах займає провідне місце. Цілком природно, що інформаційні технології, не визначаючи політику і державне управління, сильно впливають на них.

Найголовнішою якістю демократії є свобода інформації, яка сьогодні неможлива без засобів масової інформації. Нині вони настільки сильно впливають на політичне життя, державно-управлінські процеси, розвиток і функціонування демократичних принципів, що їх часто по праву

називають «четвертою владою» (поряд із законодавчою, виконавчою та судовою) [213].

Посилення функціонування засобів масової інформації неможливо без розвитку інформаційних технічних засобів. З використанням інтерактивного телебачення (телебачення зі зворотним зв'язком) ефективність засобів масової інформації зростає. Додавання до звичайного телевізора передавального пристрою з пультом зворотного зв'язку дозволяє глядачеві реагувати на запитання ведучих телепрограм, брати участь в анкетованих голосуваннях і т. ін. Створюється новий ринок замовного телебачення на екрані комп'ютера. Демократизація суспільства набуває нової якості.

Інформаційна технологія здатна підключити до активного політичного й державно-управлінського життя широкі верстви населення, виявляти громадську думку з актуальних проблем сучасності, доводити до відома громадян потрібну інформацію про діяльність державних органів, партій, громадських організацій.

Використання комп'ютерних моделей у процесі прийняття державно-управлінських рішень, не замінюючи цілеспрямованої практичної діяльності, може сприяти розкриттю альтернативних можливостей і більш обґрунтованого вибору.

Сприятливий вплив інформаційної технології на демократизацію настільки великий, що часто говорять про теледемократію – встановлення прямої демократії через підключення до засобів комунікацій.

Однак не без підстави існують й інші точки зору на співвідношення демократизації та інформатизації. Так, Т. Роззак зазначає, що комп'ютеризація сприяє підриву демократичних цінностей, попереджає, що посилюючи панування політико-управлінської еліти, нова інформаційна техніка ставить під загрозу і нашу свободу, і саме наше виживання [364, с. 14].

Деякі дослідники стверджують, що децентралізація в економічній і державно-управлінській сферах (в Україні, зокрема, найбільш активно в 2014–2019 рр. ідуть процеси децентралізації державного управління, перш за все на регіональному рівні) буде, як може здатися парадоксальним, навпаки, сприяти централізації політичної влади.

У цих умовах експлуатація нової техніки може значно посилити бюрократичні ієрархічні структури, поглибити прірву між державою та її громадянами, що призведе до формування «кібернетичної техніки правління». Все це істотно ускладнить діяльність політичної опозиції.

Автор книги «21 урок для XXI століття» відомий учений Ю. Харарі зазначає, що демократія заснована на принципі, який сформулював Авраам Лінкольн: «Можна весь час дурити деяких, можна деякий час дурити всіх, але не можна весь час обдурювати всіх». Якщо уряд корумпований і не здатний поліпшити життя людей, то рано чи пізно кількість громадян, які розуміють це, досягне критичної маси і відбудеться зміна влади. Але контроль уряду над засобах масової інформації підриває логіку Лінкольна, оскільки заважає громадянам розібратися в тому, що відбувається. Монополія в засобах масової інформації дозволяє правлячим олігархам раз по раз звинувачувати в своїх невдачах інших і переключати увагу на зовнішні загрози – реальні чи уявні [308].

У зв’язку з цим у книзі абсолютно справедливо, на нашу думку, наголошується, що основний недолік авторитарних режимів XX ст. – прагнення зосередити всю інформацію в одному місці – в XXI ст. може перетворитися на перевагу. Як тільки алгоритми навчать людей досить добре, авторитарні уряди отримають над громадянами абсолютний контроль, якого не знала навіть нацистська Німеччина, і чинити опір подібним режимам буде практично неможливо. Влада не тільки в усіх подробицях дізнається, що ви відчуваєте, – вона ще й змусять вас відчувати те, що потрібно їм. Диктатору не обов’язково гарантувати

громадянам рівність або високий рівень охорони здоров'я – йому досить вселити їм любов до себе і ненависть до своїх ворогів.

У цьому контексті можна сформулювати наукову гіпотезу про те, що демократія в її нинішній формі не переживе злиття інформаційних технологій і біотехнологій. Або демократія успішно трансформується, прийнявши абсолютно нову форму, або людям доведеться жити в умовах «цифрових диктатур». Насправді XXI ст. може породити суспільство з такою нерівністю, якого ще не знала історія. Глобалізація та Інтернет вирівнюють становище країн, але поглиблюють прірву між класами [209]. В результаті формується строго організоване суспільство, оскільки комп'ютер як важливий організаційний засіб сприятиме встановленню порядку, властивого самому комп'ютеру.

Відомий американський вчений і політичний діяч З. Бжезинський писав свого часу, що застосування інформаційної техніки в політичному управлінні суспільством призводить до формування системотехнічних методів і далі – до сістемотехнократіі як антипода демократії. Він вважав, що тенденція до сістемократії являтиме собою в майбутньому своєрідний і виклик демократичному суспільству, що постійно посилюється, з боку всіх форм і напрямків бюрократії, які ніби злилися воєдино, що полягає у вимозі більш чіткого поділу соціальних ролей і функціонуванні на основі повної технізації, автоматизації та комп'ютеризації суспільства [30–33].

Не без певних підстав можна вважати, що застосування комп'ютерів може сприяти укріпленню репресивних функцій держави, обмеженню політичної свободи громадян і, врешті-решт, встановленню «комп'ютерного тероризму». Тут ми впритул стикаємося з проблемою відкритості інформації та контролю над нею [14; 102].

Розвиток і використання в державній практиці інформаційної техніки висуває, таким чином, дві проблеми – долю демократії і контроль над людиною.

Справа в тому, що, як було показано раніше, держава володіє більшими, ніж будь-яка особистість, економічними і технічними та управлінськими повноваженнями для придбання і функціонування інформаційних засобів, воно може використовувати їх для контролю над окремими особистостями чи групами людей.

Демократичність суспільства залежить від ступеня інформованості її громадян. Однак повна свобода інформації може призвести до прямо протилежного результату – комп'ютерному контролю над особистістю, позбавлення особистої свободи. Факти свідчать, що інформаційна техніка нині широко використовується для контролю за особистістю, що підриває підвалини демократизації.

У зв'язку з цим існує загроза становлення поліцейського і політичного спостереження за індивідами за допомогою інформаційної техніки. Сучасна інформаційна техніка може бути використана для підслуховування, підглядання, перевірки банківських рахунків, станом здоров'я, стеження за подробицями інтимного життя і подальшого шантажу. Будь-яка ділова угода за наявності пластикових грошей і комп'ютеризованих торговельних угод може стати відомою.

Ми вже сьогодні живемо у світі, коли звичайний пересічна людина, перебуваючи у будь-якій точці планети, може передати й отримати будь-яку інформацію у візуальній, звуковий або текстовій формі. Це призводить до ситуації, коли індивіди все менше безпосередньо спілкуються один з одним і позбавляються значної частини того, що іменується особистим життям. Технічний прогрес у сучасних умовах дозволяє контролювати кожного власника мобільного телефону. Наприклад, сьогодні в найбільш розвинених країнах (наприклад, в Англії, Швейцарії, США та в деяких інших) не тільки розроблені, але й вже експлуатуються системи, які дозволяють відстежувати пересування людини, що має при собі стільниковий телефон, незалежно від того, чи включений він чи ні.

Контроль за інформацією найчастіше призводить до зловживань, починаючи з приховування інформації й закінчуючи її незаконним або не бажаним опублікуванням. Цей контроль з боку держави приймає все більш виражений політичний характер: так, у вересні 2019 р були оприлюднені телефонні переговори Президентів України та США В. Зеленського і Д. Трампа, що призвело до небажаних міжнародним наслідків, зокрема для України.

У зв'язку з цим російський дослідник І. Морозов вказує на парадоксальне протиріччя: ліберальний підхід до подальшого розвитку Інтернету з боку державних структур таїть у собі реальний ризик, що дана система буде використана екстремістськими силами [209]. Водночас взяття мережі під щільний і офіційний державний контроль дає владі дуже привабливий ключ до суспільства тотальної керованості. Пошук виходу з даних протиріч технологічного розвитку цивілізації, моделювання варіантів нейтралізації нових загроз, без сумніву, на наш погляд, в найближчі роки стануть важливим напрямком в науковій літературі.

Сьогодні в державно-управлінському просторі, в його принципах і правилах функціонування відбуваються радикальні зміни, воно стає все більш насиченим інформацією і вкрай динамічним. При цьому як головний системний фактор простору виступають масові політико-управлінські комунікації. Саме в межах системи масових політико-управлінських комунікацій багато в чому складається процес інформаційної взаємодії основних державно-політичних суб'єктів, реалізуються їхні політичні цілі і стратегії [214].

Слід зауважити, що формування і розвиток інформаційного політичного простору України проходить в дуже непростих умовах, стикаючись з великою кількістю проблем соціально-політичного, економічного та управлінського характеру.

На наш погляд, реформування системи державної влади і поглиблення процесів модернізації системи державного управління, при нерозвиненості системи масових політичних комунікацій і громадянського суспільства, а також постійний зовнішній інформаційний тиск уповільнюють розвиток інформаційного простору України і заважають зміцненню його цілісності та єдності, а також оптимальному включенню в глобальний інформаційний простір.

Вивчення проблеми інформаційного політико-державно-управлінського простору тісно пов'язано з аналізом місця і ролі держави в ньому як основного суб'єкта, що формує систему масових політичних комунікацій. Тільки держава, на нашу думку, здатна гарантувати громадську інформаційну свободу і захист персональних даних, забезпечувати безпеку національного інформаційного простору. Держава є центром тяжіння і перетину різних політичних комунікацій. При цьому інформаційні трансформації політичного простору змінили сутнісні риси самої держави, засоби і методи організації політичної влади, управління та контролю [237].

У зв'язку з цим актуалізуються питання статусу, який набуває держава в сучасному інформаційному суспільстві, прийнятного ступеню контролю з боку держави інформаційно-політичного простору, необхідності вжиття заходів для ефективного функціонування й підтримки центрального політичного статусу держави. Необхідно також об'єктивно оцінити, наскільки вона здатна протистояти іншим потужним інформаційно-політичним суб'єктам, наприклад, транснаціональним корпораціям, визначити, якими способами і ресурсами вона повинна володіти для встановлення політичних комунікацій і якою має бути оптимальна модель взаємодії із засобами масових комунікацій [253; 359].

Важливо з'ясувати, чи дійсно державна інформаційна політика перетворюється на ключовий спосіб керівництва та управління соціально-

політичними відносинами або ж така тенденція носить тимчасовий характер, і якою має бути ця політика, щоб, при збереженні свободи думок, було можливим рух до поставлених загальнонаціональним цілям [7; 8].

Поки що це проблемне поле розроблено досить слабо. При цьому особливо складно й суперечливо просувається справа з аналізом відповідних процесів саме в Україні, політична модернізація якої залишається актуальною, незважаючи на події 2013–2014 рр., які отримали назву «Революція гідності».

Сьогодні багато українських експертів, вчені, фахівці у сфері державно-управлінських відносин поділяють точку зору, згідно з якою нові засоби комунікацій самі по собі не допомагають розвитку демократії. Більш того, сучасні інформаційні технології породжують додаткові загрози і ризики для традиційних принципів демократії. Електронні комунікації створюють в суспільстві нові інформаційні бар'єри, «віртуальну політику», «маніпулятивну демократію» і навіть скорочують вплив суспільства на владу.

На наш погляд, в цьому контексті можна висловити гіпотезу про те, що в найближчі роки багато держав можуть зіткнутися з наближенням кризою традиційної демократії в інформаційному суспільстві, де зникає «проблема свободи слова», але виникає «проблема бути почутим». Видається, що з розвитком інформаційного суспільства відбувається «демонтаж традиційних систем управління». При цьому зворотні зв'язки в суспільстві, створювані конкуренцією масових партій, підміняються широко транслюється віртуальної політикою. Будучи позбавленим впливу на владу, суспільство перетворюється на подобу футбольних уболівальників – масово інформаційно-залучених, але не здатних змінити характер гри або реальну політику футбольного клубу.

Однак не всі експерти розцінюють ризики інформаційного розвитку як пряму загрозу демократії. Сучасні технології нерідко формують більш досконалі принципи взаємодії влади і суспільства, яких просто не існувало раніше.

Так, відомий фахівець у сфері електронних комунікацій Ю. Нісневіч указує, що «концепція "електронного уряду" – це не стільки нові технології, скільки нова філософія державного управління, що має пріоритет з акцентом на надання владою громадських послуг» [213].

Індивідуальні та масові комунікації – це не загроза демократії, а перспектива її еволюції. Можливості нових комунікацій змінюють зв'язки в суспільстві і призводять до його трансформації. Трансформація зв'язків у суспільстві, у свою чергу, веде до адекватної трансформації механізмів демократії. Нові «інформаційні загрози», на наш погляд, – це не загрози демократії, а загрози інформаційній безпеці особи та суспільства, загрози маніпулювання інформацією [344].

Можна припустити, що в сучасних умовах розширення сфери застосування інформаційних технологій здійснює складний і суперечливий вплив на сучасні суспільні процеси. З одного боку, в суспільстві виникають нові бар'єри, нові виміри нерівності та можливості для маніпуляцій. Але, з іншого боку, одночасно зміцнюється особиста інформаційна незалежність, розширюються можливості для прямої демократії.

На наш погляд, абсолютно очевидно, що розвинені країни вже усвідомлюють ризики інформаційного розвитку для демократії: «Створюючи нові канали комунікації і зміщуючи фокус уваги на нові технології, уряду, можливо, збільшують фактичний розрив в реалізації прав громадян, багато з яких не звикли або не мають можливості використовувати нові інформаційні технології» [213].

У зв'язку з цим слід мати на увазі, що суперечності, пов'язані з впливом інформаційних технологій у державно-управлінській сфері різних держав, можуть призвести до реальної загрози політичної стійкості держави, а в науковому сенсі формують «політолого-інформаціологічну» проблему, яка виражається в протиріччі цілей політичного розвитку, інформаційно-комунікативних принципів політичної модернізації, інноваційної моделі державного управління і традиційного домінування механістичної, маніпулятивної моделі в системі «суспільство – ЗМІ – влада», яка виключає використання діалогових, комунікативних механізмів у прийнятті політичних рішень, що, в свою чергу, стримує процес реформування і якісні зміни управлінського середовища [96, с. 16].

Проте, як нам видається, ми є свідками того, що кількісна і якісна інтенсифікація комунікаційних процесів у державно-управлінських відносинах і як наслідок – освоєння комп'ютерних технологій породила принципово новий вектор впливу на характер соціально-політичного і управлінського розвитку соціуму. З появою Інтернету виникло нове, універсальне, інтерактивне інформаційне середовище, розвивається за своїми законами і все наполегливіше заявляє про себе як про незамінний елемент сучасної політичної системи демократичного типу.

Підвищення рівня оперативності обміну інформацією, її доступності та «прозорості» рівною мірою для всіх акторів державно-політичного процесу, унікальна можливість генерувати інформаційні потоки в обхід фільтрації з боку державних структур – всі ці очевидні й досить глибоко обговорювані української політико-управлінської наукою потенційні ресурси Інтернету традиційно розглядаються як один із векторів демократизації політичної системи посттоталітарних суспільств [351].

Однак, як нам уявляється, питання безпеки, якісно нові виклики і загрози, пов'язані з інформаційними потоками всередині політично-управлінської системи, при побудові наукових теоретичних моделей

інформаційного (постіндустріального) суспільства, занадто часто витісняються на задній план.

У зв'язку з цим не слід забувати, що інформаційні технології здійснюють двоякий вплив на сучасний державно-політичний процес. З одного боку, спостерігається позитивна динаміка їх впливу на людину і суспільство, а з іншого – проявляються негативні тенденції, що відображають як складний характер взаємодії людини з новими комп'ютерними системами, так і спроби використовувати їх потенціал для пропаганди насильства, тероризму, людиноненависницької моралі.

В сучасних умовах з'явився спектр нових інформаційних загроз, які здійснюються за допомогою спеціально підібраної системи інформації і спрямованих на дестабілізацію суспільства. У державно-управлінській сфері з'являються нові можливості для маніпулювання суспільною свідомістю, політичними настановами та орієнтаціями різних соціальних груп.

Технологічні досягнення, їх широке проникнення і фактична доступність ведуть до формування особливого світовідчуття. Віртуальна реальність істотно трансформує сучасну політичну та державно-управлінську реальність.

Таким чином, наслідки проникнення інформаційних технологій у традиційні моделі взаємовідносин у сфері політики і державного управління неоднозначні й суперечливі. З одного боку, інформаційні технології сприяють формуванню більш досконалих, таких, що не існували раніше, принципів взаємодії влади і суспільства. За допомогою електронних пристроїв зміцнюється особиста інформаційна незалежність, розширюються можливості для конвенційної участі людей в політико-управлінському процесі. З іншого – інформаційні технології породжують додаткові загрози і ризики для традиційних принципів демократії і державного управління. У суспільстві виникають нові інформаційні

бар'єри, нові виміри нерівності, «віртуальна політика», «віртуальне управління» і «маніпулятивна демократія» [209].

Підбиваючи проміжні підсумки, можемо зробити такі висновки.

1. Електронні засоби масової інформації та Інтернет відіграють все більшу роль у політичних і державно-управлінських процесах. У зв'язку з інтенсивною інформатизацією державно-управлінських відносин, політичного процесу вельми актуальною стає проблема забезпечення інформаційної безпеки в цій сфері.

2. У теоретичному плані розгляд проблем інформаційної безпеки державно-управлінської сфери тісно пов'язаний з проблемою співвідношення інформатизації суспільства з його демократизацією.

3. Багато фахівців відзначають, що останнім часом стає все більш очевидною загроза поліцейського і політичного спостереження за індивідами за допомогою інформаційно-комунікаційних технологій.

4. Сьогодні спостерігається парадоксальна суперечність: ліберальний підхід до подальшого розвитку Інтернету з боку державних структур містить у собі реальний ризик, що ця система буде використана дезінтеграційними та екстремістськими силами. Водночас взяття мережі під щільний і офіційний державний контроль дає владі дуже привабливий ключ до суспільства тотальної керованості. Пошук виходу з даних протиріч технологічного розвитку цивілізації, моделювання варіантів нейтралізації нових загроз, без сумніву, в найближчі роки стануть важливим напрямком в науковій думці, в тому числі й у сфері державного управління.

Висновки до другого розділу

Розвиток інформаційних процесів на сучасному етапі розвитку цивілізації супроводжуються не просто технологічною, а

соціотехнологічною революцією, в ході якої формується новий домінуючий тип соціальної організації – інформаційне суспільство. Вітчизняні та зарубіжні вчені сходяться на думці, що постіндустріальне суспільство має інформаційну й мережеву природу, в основі якої лежить комплексне, різнобічне знання й вільне поширення пов'язаної з ним інформації за допомогою мережевої інформаційно-комунікаційної інфраструктури.

У даний час постіндустріальне інформаційне суспільство вже стає об'єктивною реальністю для провідних держав світу, траєкторії розвитку яких розміщуються в постіндустріальному цивілізаційному коридорі, а для інших країн, перш за все з перехідною економікою, які мають інші траєкторії соціально-економічного й політичного руху, – основним орієнтиром розвитку.

У розвинених країнах і у більшості країн, що розвиваються, де пріоритетність інформаційного розвитку як ключового чинника, що визначає місце країни у світовому співтоваристві, давно усвідомлена, розроблені та реалізуються різні стратегії або комплексні програми інформаційного розвитку. Незважаючи на істотні відмінності таких стратегій і програм у країн-членів Європейського Союзу, Балтійського регіону Європи, Японії, США, Індії, Бразилії, Мексики, вони мають і яскраво виражені загальні тенденції. Їх основна мета – досягнення лідерства в економіці, соціальному розвитку, державному управлінні. Всі мережеві технології, що використовуються в них (електронний бізнес, електронний уряд, електронна демократія і т. ін.), розглядаються не як ізольовані сфери діяльності, а як інтегрований і взаємопов'язаний комплекс, єдина соціо-технологічна основа сучасного інформаційного середовища, фундамент переходу до інформаційного суспільства.

В усіх стратегіях відзначається провідна роль держави в процесі інформаційного розвитку, в консолідації всіх верств суспільства на основі

партнерських відносин між учасниками цього процесу і координації спільної діяльності держави, бізнесу, громадських інститутів і громадян для досягнення національних цілей такого розвитку.

Водночас світовий досвід засвідчує, що інформаційний розвиток з метою переходу до інформаційного суспільства, як і будь-який новий цивілізаційний феномен, породжує комплекс нових загроз і можливих негативних наслідків як внутрішньополітичного, так і геополітичного характеру. У різних країн і соціальних груп існують різні можливості доступу до світових інформаційних ресурсів, що породжує «цифрову нерівність» як на внутрішньо-, так і на міждержавному рівні [107].

Поляризація світу і зростаючий розрив між багатими і бідними, технологічно просунутими й відсталими країнами створюють нові джерела нестабільності, нинішніх і майбутніх конфліктів, в тому числі глобального характеру.

Інформаційні технології є важливим фактором інформатизації державно-управлінських відносин і забезпечення інформаційної безпеки держави. У державному управлінні інформаційні технології виступають як комплекс інформаційних середовищ, які керують владних структур, політичних інститутів, громадян, що утворюють цілісну систему, пов’язану з допомогою інформаційних потоків із зовнішніми по відношенню до політики суспільними процесами [108].

В умовах інформатизації продовженням розвитку загальної теорії демократії є поява концепції «електронної демократії». Однак існуючий розрив між потенційними можливостями, що випливають з даної концепції, і практичною реалізацією її ідей, обумовлений неоднозначним розумінням її суті науковими колами, політично-управлінськими елітами і громадянами, а також принципово різними інтересами учасників управлінського процесу щодо цілей її практичної реалізації.

Включення Інтернету в процеси інформаційної взаємодії у сфері політики і державного управління стало можливим завдяки усвідомленню політичними й управлінськими акторами потенційних можливостей мережі. Технологічні інновації якісно змінюють інформаційне середовище існування державного управління, політичного процесу, сприяючи наданню їм властивостей віртуальності, інтерактивності, глобальності, пов'язаності, стійкості. Постійні технологічні зміни в Інтернеті провокують появу нових політично-управлінських практик.

Аналіз Інтернету як політичної технології, яка застосовується на різних стадіях політичного процесу, починаючи з кінця 90-х рр. XX ст., дозволяє говорити про поступове зростання масштабів мережевої політично-управлінської активності всіх учасників управлінського процесу. Переміщення політичної активності в мережу призводить до зміни основ існування самої державної політики.

Активне освоєння Інтернету політичними учасниками призводить до формування глобального політично-управлінського ринку, на якому вільно поширюється продукція будь-якої політичної спрямованості. Відбувається формування глобальних політичних спільнот і організацій, що не мають національно-державних юрисдикції.

Для України XXI ст. просування до інформаційного суспільства стає важливим геополітичним фактором і має стати основою довгострокової стратегії соціально-економічного розвитку країни та забезпечити суттєве підвищення якості життя населення. Тільки в цьому випадку Україна зможе інтегруватись у світовий економічний простір як сильний і рівноправний партнер, який повною мірою використовує конкурентні переваги «нової» економіки, що спирається на інформацію і знання.

Характеризуючи ситуацію в цілому, можна стверджувати, що зміна соціальних орієнтирів і цінностей й даний час активізує потреби людей в соціально значимій інформації для орієнтування в політичній і соціально-

економічній ситуації на центральному, регіональному та місцевому рівнях. Це змушує їх стати активними споживачами інформації, учасниками інформаційно-комунікативних процесів в українському суспільстві.

Зазначені явища протікають в умовах бурхливого розвитку інформаційних технологій, засобів телекомунікації та обробки інформації, що робить інформаційно-комунікативні процеси ключовим фактором державного управління. Інформаційно-комунікативні процеси є своєрідною процесуальною складовою інформаційних правовідносин й активно впливають на індивідуальну, групову та суспільну психологію (індивідуальну, групову й масову свідомість) [258].

Інформаційні потоки, які направляють на людину засоби масової інформації, не тільки освічують і беруть участь в її орієнтації в сучасному світі, але в цілому формують її духовний статус, психологічний простір, емоційний тонус, градус її відносин з реальністю та оточуючими, впливають на її самопочуття у світі і суспільстві.

З огляду на це можна дійти висновку про необхідність аналізу потреб реального життя в ефективному забезпеченні інформаційно-психологічної безпеки особи, суспільства і держави, перебудови чинного правового механізму, покликаного забезпечити належний захист інтересів особи, суспільства і держави в інформаційній сфері.

Сформована система забезпечення інформаційної безпеки в сучасній Україні наразі не здатна, на наш погляд, протистояти сучасним загрозам. Просування нашої країни до інформаційного суспільства передбачає ефективний захист національних інтересів в інформаційній сфері, реалізацію основних положень Доктрини інформаційної безпеки України. При цьому мають бути вирішені завдання забезпечення інформаційної безпеки об’єктів інформаційної сфери, насамперед національних інформаційних ресурсів, інформаційно-комунікаційної інфраструктури країни, систем і засобів телекомунікації та зв’язку в життєво важливих

сферах функціонування суспільства і держави. Крім того, необхідно створити ефективну систему координації діяльності різних організацій і відомств у сфері забезпечення інформаційної безпеки.

РОЗДІЛ 3
ОЦІНКА СУЧАСНОГО СТАНУ ТА ПЕРСПЕКТИВ РОЗВИТКУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ

3.1. Закордонний досвід розроблення та впровадження інформаційного забезпечення державної безпеки

Досвід провідних країн переконливо доводить, що розвинені система комунікацій та інформаційні технології виявляються досить прибутковими. Фактом є і те, що держави з розвинутою системою інформаційних комунікацій автоматично стають частиною глобального інформаційного суспільства.

Розглянемо детальніше деякі тенденції, що спостерігаються в різних країнах у сфері розроблення та використання інформаційного забезпечення державної безпеки.

Першу спробу комплексно розглянути проблеми інформаційної безпеки на міжнародному рівні здійснила Організація економічного співробітництва та розвитку у 1986 році. Зокрема, вона рекомендувала за результатами роботи свого правового комітету віднести до кримінально караних такі дії:

– зміна комп’ютерних даних з метою незаконного збагачення;

– зміна комп’ютерних даних з метою підроблення;

– зміна комп’ютерних даних з метою порушення функціонування комп’ютерів;

– порушення авторського права на комп’ютерні програми з метою отримання прибутку;

– доступ до комп’ютера або перехоплення інформації без дозволу відповідальної особи шляхом порушення охоронних заходів.

Динаміка поширення комп'ютерної злочинності підштовхнула Раду Європи − іншу міжнародну організацію – у межах боротьби з цим негативним явищем зайнятися розробленням та узгодження підходів до створення відповідних кримінально-правових приписів. Зокрема, Комітет Міністрів країн-членів Ради Європи у 1989 році такий рекомендаційний перелік злочинів у розглядуваній сфері:

– комп'ютерне шахрайство;

– комп'ютерне підроблення;

– комп'ютерний саботаж;

– несанкціонований доступ до інформації;

– неправомірне відтворення виробів і програм, які охороняються авторським правом.

У 2001 р. Рада Європи ухвалила Європейську конвенцію про кіберзлочинність (інформаційну безпеку), в якій до кримінальних злочинів було зараховано такі групи суспільно небезпечних діянь проти конфіденційності даних:

– протиправний доступ;

– перехоплення;

– порушення цілісності;

– втручання в роботу;

– виробництво, обіг та використання спеціальних засобів для вчинення комп'ютерних злочинів з використанням комп'ютерів;

– підроблення інформації;

– інформаційне шахрайство тощо.

Узгодження різнопланових і різноспрямованих міждержавних підходів до кримінальної відповідальності за вчинення злочинів в інформаційній сфері відбувалося і під час розробки Модельного кримінального кодексу для країн-учасниць СНД, який був ухвалений у 1996 р. У цьому міжнародному документі встановлювалася кримінальна відповідальність за такі суспільно небезпечні діяння проти інформаційної безпеки:

– несанкціонований доступ;

– модифікація інформації;

– виготовлення засобів доступу до інформації;

– розроблення шкідливих програм;

– порушення правил експлуатації комп'ютерів;

– порушення правил поводження з документами, які містять таємницю.

Також країни-учасниці СНД підписали угоду про співробітництво в галузі забезпечення інформаційної безпеки.

Втім, в умовах стрімкого поглиблення інформатизації суспільства норми міжнародно-правового режиму інформаційної безпеки виявились недостатньо повними, і міжнародне співтовариство цей факт уже визнало.

У межах ООН триває активний переговорний процес щодо правового режиму інформаційної безпеки. Пов'язані з ним проблеми обговорювалися на всіх сесіях Генеральної Асамблеї ООН. Головними питаннями є такі:

– визначення основних понять інформаційної безпеки;

– створення міжнародної системи моніторингу загроз цій безпеці;

– розроблення міжнародно-правового режиму такої безпеки;

– підготовка договору про боротьбу з інформаційним тероризмом;

– запобігання появі нової інформаційної сфери конфронтації;

– формування загальних поглядів на використання інформаційних технологій як зброї;

– оцінювання руйнівних властивостей шкідливих програм для критично важливих елементів інфраструктури держави;

– відмова від дезінформації з метою руйнування духовного середовища.

Вирішення цих проблем дозволить покращити загальний рівень міжнародної інформаційної безпеки. В Окінавській хартії глобального інформаційного суспільства й актах Шанхайської організації співробітництва окремо підкреслюється необхідність посилити нормативну базу, що регулює інформаційні відносини. Тим не менш, реального просування у сфері

державного регулювання інформаційної безпеки, серед іншого тоді, коли доводиться вирішувати транскордонні правові проблеми, вдасться досягти, якщо спиратися на практичний досвід повсюдного застосування міжнародних стандартів інформаційної безпеки.

Цікавість з боку науковців і практиків до питань ефективного держуправління інформаційними системами і технологіями стимулювало швидкий розвиток багатьох галузевих, національних і міжнародних стандартів як управління цими технологіями і системами взагалі, так, зокрема, і їх безпекою. Так, у публікації Американського Інституту Дипломованих Бухгалтерів було показано, що останніми роками під поняттям «інформаційна безпека» найчастіше розуміють апаратні засоби, програмне забезпечення, процеси та процедури, об'єднані для захисту інформаційних систем організації від внутрішніх і зовнішніх загроз. Ця дефініція стала в США темою номер один у сфері технологій. Унаслідок високої динаміки сучасних бізнес-процесів просто бракує часу для розроблення нових вітчизняних технологій, тому краще віддавати перевагу активному застосуванню найбільш вдалих світових практик, до яких належать і стандарти інформаційної безпеки [64; 77].

Стандарти управління і безпеки інформаційних технологій розроблялися на підставі аналізу й узагальнення кращих методів, перевірених та апробованих як великими групами професіоналів, так і безліччю різних організацій. Кращі стандарти управління і безпеки цих технологій наразі теж не є результатами суто наукових досліджень.

У першій половині XX століття, коли масово винаходилися і швидко починали широко використовуватися різноманітні електроприлади, для поліпшення умов міжнародної торгівлі та її кращого убезпечення були розроблені й невдовзі отримали загальне визнання міжнародні стандарти щодо електричних приладів. Це призвело до створення Міжнародної Електротехнічної Комісії. Набагато пізніше, з появою потреби у міжнародних стандартах в інших галузях, насамперед щодо якості, була

заснована Міжнародна Організація по Стандартизації (англ. – International Organization for Standardization − ISO). Оскільки комп'ютер і телекомунікаційні системи вимагають уваги як до електротехнічним питань, так і до питань якості, International Electrotechnical Commission об'єднала свої зусилля з розроблення відповідних стандартів у Joint Technical Committee.

На додаток до згаданих міжнародних стандартів існує багато національних стандартів щодо управління і безпеки інформаційних технологій. Наприклад, якщо в США і низці інших країн для управління інформаційними технологіями найчастіше використовуються Control Objectives for Information and related Technology (COBIT), то у Великобританії, Нідерландах та Австралії – IT Infrastructure Library (ITIL). Більшість країн має власні організації, які розробляють стандарти для різних випадків. Це можна пояснити тією обставиною, що найкраща з описаних практик для конкретних умов нерідко буває доступною чи взагалі застосовною лише в місцевому масштабі.

Бажання управляти проєктами у відповідності до кращих практик призвело до виникнення методу управління проєктами «Проєкти в контрольованому середовищі» (англ. Projects in Controlled Environments – PRINCE) в Європі та Довідника з управління проєктами (англ. − A Guide to the Project Management Body of Knowledge або PMBOK Guide) в США. Так сталося незважаючи на те, що управління проєктами не дуже сильно відрізняється на різних континентах.

Оскільки стандарти є результатом обговорення особистостей, то розходження ідей, культурних, політичних і національних особливостей, вели і будуть завжди вести до швидкого зростання кількості локальних стандартів.

Для окремої організації було б надзвичайно важко придумати кращу структуру управління інформаційними технологіями ніж COBIT або ITIL. Крім того, більшість законодавчих актів (типу Акту Sarbanes-Oxley в США і

Tabaksblat в Нідерландах) зобов'язують організації, до яких ці акти належать, застосовувати кращі практики.

Найбільші організації вже зрозуміли, що створення власних політик інформаційної безпеки часто набагато дорожчі та менш успішні, ніж опора на ISO 17799. Інші вигоди від використання стандартів управління і безпеки інформаційних технологій стають очевидними тоді, коли організація вирішує віддати частину своїх функцій на аутсорсинг. Застосування відкритих стандартів як основу під час укладання угод про рівень обслуговування між партнерами призводить до зменшення розбіжностей і зниження супутніх витрат і ризиків.

Якщо в минулому аудитори створювали власні набори стандартів, програми аудиту і контрольні списки для використання їх як еталонів, то тепер використання публічно доступних міжнародних стандартів (типу COBIT, ISO 17799 та ISO 9001) призводить до зниження витрат як для аудитора, так і організації, що підлягає аудиту, і допомагає організаціям краще розуміти аудиторів.

Організації також можуть використовувати відкриті стандарти і для внутрішнього аудиту, створюючи тим самим базу для інтегрованого аудиту. Навіть сам процес аудиту був стандартизований такими міжнародними стандартами як ISO 19011 і EA 7/03.

Посилення уваги до якості корпоративного управління призводить до зростання значимості незалежної сертифікації. Швидке оцінювання бажаності ведення торгівлі з організацією без зовнішнього аудиту, що дорого коштує, або перевірки спрощується, якщо ця організація може довести відповідність критеріям, пред'являючи свідоцтва від зовнішньої, незалежної сторони, яка заздалегідь оцінила якість і безпечність цієї організації.

Для таких стандартів, як BS 15000 (англ. British Standards), ISO 9001, стандарти Європейського Фонду Управління Якістю і TickIT, також існують процедури сертифікації.

Для цілей аудиту інформаційних систем (тобто управління інформаційними технологіями, безпеки, планування безперервності бізнесу і самого процесу аудиту), найбільш цікавими є такі процедурні стандарти:

– управління інформаційними системами: COBIT, BS 15000, Microsoft Operations Framework і ITI (англ. – Information Technologies Institute);

– управління проєктами: PRINCE2 і the PMBOK;

– управління безпекою: ISO 13335, ISO 13569 (банківські і фінансові послуги), ISO 17799/BS 7799-2 (обидва локалізовані для багатьох країн), IT Baseline Protection Manual (Німеччина), ACSI-33 (Австралія), безліч стандартів National Institute of Standards and Technology;

– управління якістю: ISO 9001, EFQM і Baldrige National Quality Plan;

– програмування: TickIT, Capability Maturity Model Integration – стандарти корпоративного управління інформаційними і комунікаційними технологіями;

– управління ризиками − Австралійський стандарт AS/NZS 4360;

– планування безперервності бізнесу: British Standards Institution PAS-56 і Австралійський стандарт HB 221-2004;

– аудит інформаційних систем − COBIT та ISO 19011.

Крім великої кількості процесуальних і тактичних стандартів (тобто, стандартів щодо процесів і процедур), існує ще більша кількість експлуатаційних, технічних стандартів. Зокрема, такі організації, як Міжнародна організація зі стандартизації, Європейський Інститут Стандартів Телекомунікації та Національний Інститут Стандартів і Технології запровадили стандарти стосовно шифрування, технічні критерії оцінювання безпечності інформаційних технологій, планування безперервності бізнесу та використання паролів.

Зокрема, серед стандартів управління безперервністю бізнесу ключовими вважаються Publicly Available Specification 56 (розроблений Британським Інститутом Стандартів) і Handbook 221 (Business Continuity Management від Standards Australia). Вони описують стратегічні та

експлуатаційні підходи, покликані протистояти порушенням, перервам або втратам під час виробництва виробів і надання послуг. Передбачені в цих стандартах процеси не вкладаються в межі самого лише планування дій у надзвичайних ситуаціях.

Саме через стандарти, які не є адекватними ситуації, нерідко ініціюють дорого вартісні проєкти, не здатні забезпечити досягнення поставлених цілей. Найкращі стандарти зазвичай залишають простір для їх інтерпретації, однак остання іноді стає причиною появи нових проблем. Зокрема, стандарт на кшталт ISO 17799 роз'яснює, що таке безпека, але не як можна забезпечити такий стан.

Деякі із зазначених вище стандартів об'єднуються у так звані сімейства стандартів чи вступають їх складовими частинами. Наприклад, BS 15000, британський стандарт для управління послугами у сфері інформаційних систем, складається з двох частин. Перша є специфікацією для управління послугами, а друга містить низку правил для управління цими послугами. Ще нижче в цій ієрархії перебуває ITIL, у якому зібрано кращі практики для процесів, описаних у BS 15000, і, більш того, внутрішні процедури організації цих процесів. Схожа ієрархія зустрічається у таких стандартах:

– BS 7799-2 (специфікація управління інформаційною безпекою);

– ISO 17799 (набір кращих практик управління інформаційною безпекою);

– ITIL Security Management (опис процесів інформаційної безпеки).

У разі існування такої великої кількості стандартів державного регулювання інформаційної безпеки професіонали повинні мати в своєму арсеналі їх вибір. Для їх правильного застосування виникає потреба створити карти сфер їх застосовності та зв'язків між ними. Це може призвести до появи метастандарту − стандарту стандартів. На жаль, такого метастандарту поки що не існує. Більшість згаданих стандартів присвячено властивостям тих або інших процесів. Технічні стандарти, типу ISO 15408 та критерії

оцінювання безпеки інформаційних технологій описують необхідні властивості систем більш докладно.

Управління інформаційними системами пов’язується з внутрішніми і короткостроковими оперативними бізнес-проблемами, тоді як корпоративне управління такими системами зосереджується на зовнішніх довгострокових бізнес-перспективах.

IT Governance Implementation Guide з високим ступенем деталізації описує кроки з впровадження корпоративного управління інформаційними технологіями.

У грудні 2000 року перша частина Британського Стандарту 7799 стала стандартом ISO 17799, який охоплює більше тисячі найкращих практик управління безпекою, зокрема інформаційною, які обєднано у 127 параграфів. Багато країн цей стандарт не задовольнив, що було зрозуміле ISO, і тому терміново було розпочато створення проєкту його перегляду, внаслідок чого того ж року світ побачила покращена модифікація стандарту ISO 17799.

На відміну від першої, друга частина BS 7799 не належала до стандартів ISO. Там були присутні ті ж самі 127 параграфів, але в нормативній формі, а головне – саме там міститься опис циклу «план − здійснення − перевірка − дія» стосовно управління інформаційною безпекою. Видана у 2002 р. версія BS 7799 уже повністю відповідала стандартами якості ISO, а згодом другу частину цього стандарту було перетворено на міжнародний стандарт управління безпекою ISO.

У свою чергу цей документ також має дві частини, на відміну від «технічного звіту», який містить дані, що зовні відрізняються від зазвичай використовуваних у міжнародних стандартах управління безпекою інформаційних і телекомунікаційних технологій.

Технічний звіт ISO 13569 «Банківські та супутні фінансові послуги − керівні принципи інформаційної безпеки» теж збиралися переглянути. Він забезпечив керівними принципами проєкти розвитку інформаційної безпеки

в індустрії фінансових послуг. Цей стандарт охоплює політичні, організаційні, структурні, юридичні та регулюючі компоненти таких проєктів [44].

Визнаючи важливість інших широко визнаних стандартів крім COBIT, IT Governance Institute розробив структуру для порівняння стандартів і колекцій кращих практик. Він використав цю структуру для високорівневого порівняння ряду стандартів управління інформаційними технологіями, інформаційною безпекою та якістю з COBIT. Відповідно, було опубліковано детальне порівняння методів управління COBIT з ISO 17799. Інші організації також робили спроби позиціонування різних стандартів. Так, Німецький федеральний офіс з інформаційної безпеки порівнював свій стандарт управління безпекою інформаційних технологій Baseline Protection Manual з ISO 17799.

Наприкінці зауважимо, що чинні наразі міжнародні стандарти державного регулювання інформаційної безпеки висвітлюють окремі його аспекти. Дійсно, ISO 17799 згадує про важливість аудиту інформаційної безпеки, однак не містить жодної інформації щодо його здійснення. Тут можуть використовуватися керівні принципи аудиту COBIT, особливо в тих умовах, коли COBIT активно порівнюється з ISO 17799. Процес стратегічного управління інформаційною безпекою описано в BS 7799, а оперативну складову управління безпекою інформаційних технологій – у Security Management ITIL. Професіонали повинні бути здатні будувати систему управління безпекою, використовуючи найкращий із цих стандартів [44].

3.2. Організаційно-правові механізми інформаційного забезпечення державної безпеки

Нині в Україні активно формується інформаційне суспільство, і ця обставина породжує нові вимоги до інформаційно-комунікативної функції

держави. Зокрема, реалізація цієї функції викликає посилення уваги до проблемних питань щодо пошуку компромісу між інтересами особи, суспільства та держави в інформаційній сфері. В умовах цивілізованої держави ці інтереси вочевидь мають регламентувати відповідні нормативно-правові акти.

Зауважимо, що в Україні законодавча база, покликана регулювати суспільні відносини в розглядуваній сфері, перебуває в стадії становлення. Як позитивний момент можна виділити тенденції, що намітилися у сфері вдосконалення нормативно-правового забезпечення реалізації інформаційно-комунікативної функції держави.

Спочатку необхідно визначити коло інтересів особи, суспільства та держави в зазначеній сфері, чим фактично задається основний напрямок подальшого правового забезпечення державного регулювання інформаційно-комунікативних процесів.

Зокрема, в цій сфері існують такі інтереси особи:

– реалізація конституційних прав людини і громадянина на доступ до інформації;

– використання інформації для здійснення будь-якої не забороненої законом діяльності, а також фізичного, духовного й інтелектуального розвитку особи;

– захист інформації, що забезпечує особисту безпеку.

Інтереси суспільства в цій сфері є такими:

– забезпечення інтересів особи (див. вище);

– зміцнення демократії;

– розбудова правової соціальної держави;

– досягнення злагоди в суспільстві та її підтримання;

– духовне оновлення нашої держави.

Інтереси держави у цьому є такими:

– створення в Україні умов для подальшого формування гармонійної інформаційної інфраструктури;

– реалізація передбачених Конституцією прав і свобод людини і громадянина стосовно одержання інформації і користування нею з метою забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності й досягнення політичної, економічної та соціальної стабільності в Україні;

– забезпечення законності та правопорядку;

– налагодження рівноправного і взаємовигідного міжнародного співробітництва.

Незважаючи на певне коло інтересів в інформаційній сфері, у вітчизняній юридичній науці повною мірою не склався єдиний підхід до питань, що стосуються системи інформаційного законодавства, що природно ускладнює і дослідження нормативно-правової бази реалізації розглядуваної функції держави.

Швидше за все під час формування законодавства в інформаційній сфері його частина, присвячена забезпеченню інформаційної безпеки, виступає підгалуззю інформаційного законодавства, а під час його кодифікації, у разі ухвалення Інформаційного кодексу України, може стати його складовою частиною. Але становлення інформаційного законодавства як окремої галузі українського законодавства є справою важкою, розрахованою, мабуть, на довгі роки.

Уже сьогодні всю систему чинних нормативно-правових актів, базових для реалізації інформаційно-комунікативної функції держави, умовно можна розглядати як трирівневу систему (по вертикалі), що охоплює:

– рівень міжнародного права;

– конституційний рівень;

– рівень поточного внутрішньодержавного законодавства.

Водночас зазначена нормативно-правова база може розглядатися і у функціональному аспекті (по горизонталі), наприклад, як підсистем нормативно-правових актів, що забезпечують реалізацію прав і інтересів особи, суспільства і держави за такими напрямами:

– вільний доступ до масової інформації та вільний інформаційний обмін нею;

– захист визначених законом видів інформації від несанкціонованого доступу;

– захист особи та суспільства від деструктивного інформаційного впливу.

З аналізу нормативно-правової бази реалізації розглядуваної функції держави випливає, що, попри наявні прогресивні зрушення, законодавство, що розглядається, не можна назвати розвиненим, бо воно суперечливе, здебільшого має декларативний характер, має суттєві прогалини. Усе це створює юридичні бар'єри на шляху реалізації державою інформаційно-комунікативної функції.

Нижче зазначені вище особливості розглянуто більш докладно.

Так, що стосується суперечливості, то суперечності закладено навіть у чинних базових законах:

– Закон України «Про інформацію» від 02.10.1992 № 2657-XII;

– Закон України «Про телекомунікації» від 18.11.2003 № 1280-IV;

– Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII;

– Стратегія національної безпеки України;

– Стратегія кібербезпеки України;

– Доктрина інформаційної безпеки України;

– Воєнна доктрина України;

– Стратегічний оборонний бюлетень України.

Зокрема, базовий стосовно інформаційної безпеки Закон України «Про інформацію» від 02.10.1992 № 2657-XII оголошує її забезпечення одним із напрямів державної інформаційної політики (ст. 3 «Державна інформаційна політика»).

У свою чергу, Закон України «Про телекомунікації» від 18.11.2003 № 1280-IV розглядає забезпечення інформаційної безпеки в контексті

забезпечення надійності та безпеки телекомунікаційних мереж (ст. 24 «Умови застосування технічних засобів телекомунікацій»).

Закон України «Про основні засади забезпечення кібербезпеки України» закріплює правові й організаційні засади забезпечення захисту життєво важливих інтересів людей, громади, суспільства і держави, а також національних інтересів України у межах кіберпростору. Крім того, цей закон визначає:

– ключові цілі, напрями та принципи державної політики у напрямі забезпечення кібербезпеки;

– повноваження органів державної влади та місцевого самоврядування, підприємств, організацій, установ, громадян та інших осіб стосовно забезпечення кібербезпеки;

– ключові основи координації діяльності органів державної влади та місцевого самоврядування з громадськістю стосовно забезпечення кібербезпеки.

Стратегія національної безпеки України була затверджена Указом Президента України від 26.05.2015 № 287/2015 «Про рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України"». У ній описано загрози інформаційній безпеці (підпункт 3.6 розділу 3 «Актуальні загрози національній безпеці України»).

Стратегію кібербезпеки України було затверджено Указом Президента України від 15.03.2016 № 96/2016 «Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України"». Серед іншого зазначено такі її пріоритети:

– формування вітчизняної нормативно-правової бази та впорядкування термінології, що стосується інформаційної безпеки;

– уніфікація нормативних документів, присвячених електронним комунікаціям;

– захист інформації та інформаційної безпеки, зокрема кібербезпеки, відповідно до міжнародних стандартів і стандартів ЄС та НАТО [259].

Доктрину інформаційної безпеки України затверджено Указом Президента України «Про рішення Ради національної безпеки і оборони України від 25.02.2017 № 47/2017 “Про Доктрину інформаційної безпеки України”». У ній зафіксовано:

– національні інтереси України щодо інформаційної сфери;

– загрози реалізації національних інтересів щодо захисту інформації;

– пріоритети і напрями державної політики в інформаційній сфері.

Зауважимо також, що деякі питання інформаційної безпеки, наприклад стосовно комерційної таємниці, досі чітко не врегульовано.

Так, у статті 21 Закону України «Про інформацію» від 02.10.1992 № 2657-XII міститься дефініція інформації з обмеженим доступом, якою, зокрема, визнається конфіденційна, таємна та службова інформація.

У свою чергу, різні правові галузі передбачають наявність таких видів інформації з обмеженим доступом:

– державна таємниця – Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII;

– інформація про особу – Закон України «Про інформацію» від 02.10.1992 № 2657-XII;

– комерційна інформація (таємниця) – стаття 505 Цивільного кодексу України від 16.01.2003 № 435-IV;

– адвокатська таємниця – Закон України «Про адвокатуру» від 05.07.2012 № 5076-VI;

– лікарська таємниця – Закон України «Основи законодавства про охорону здоров’я» від 19.11.1992 № 2801-XII;

– таємниця листування, проведення телефонних розмов, телеграфної й іншої кореспонденції – Конституція України;

– таємниця усиновлення – стаття 228 Сімейного кодексу України від 10.01.2002 № 2947-III;

– таємниця страхування – Закон України «Про страхування» від 7.03.1996 № 85/96-ВР;

– банківська таємниця – Закон України «Про банки і банківську діяльність» від 7 грудня 2000 № 2121-III;

– професійна таємниця – Закон України «Про рахункову палату» від 2.07.2015 № 576-VIII;

– таємниця слідства – Закон України «Про оперативно-розшукову діяльність» від 18.02.1992 № 2135-XII;

– таємниця сповіді – Закон України «Про свободу совісті та релігійні організації» від 23.04.1991 № 987-XII.

При цьому, наприклад, в різних нормативних актах перелічується велика кількість таємниць, проте за розголошення не всіх із них передбачається відповідальність, тобто деякі норми є суто декларативними.

Також варто звернути увагу на те, що сучасне українське законодавство, яке регулює питання забезпечення інформаційної безпеки, не розглядає таку безпеку у форматі захисту інформаційної свободи.

Крім того, недосконаліть правової бази є природною в період, коли суспільні відносини випереджають законодавчу базу, через що громадяни, суспільство, підприємства й організації змушені самі захищати свої права, нерідко порушуючи задекларовані законами норми.

У цілому сьогодні слід визнати відсутність єдиного правового поля, коли норми законів суперечать Конституції, а підзаконні акти як і раніше є основою для свавілля чиновників. Держава, будучи не в змозі в повному обсязі впоратися із завданням забезпечення безпеки всіх суб'єктів інформаційних відносин, змушує їх реалізовувати свої інтереси і захищати свої права самотужки й усіма способами, не забороненими законом, відповідно до конституційного принципу самозахисту. Однак держава в більшості випадків, не врегламентувавши ці заборони на законодавчому рівні, намагається в особі різних структур дозволяти такий захист в кожному конкретному випадку.

Зокрема, залежно від визначеного виду інформаційних відносин, які підлягають інформаційному впливу, органи державної влади спеціальної компетенції можна поділити на такі:

– органи, які прямо впливають на сферу інформаційних відносин у загальному контексті та провадять державну інформаційну політику (Державний комітет телебачення і радіомовлення України);

– органи, що розробляють і провадять державну мовну політику та державну політику із захисту суспільної моралі (Міністерство культури України);

– органи, що в той чи інший спосіб регулюють отримання і зберігання інформації (Державний комітет статистики України та Державний комітет архівів України);

– органи, що відповідають за аналіз і моніторинг певних типів інформації (Державна служба фінансового моніторингу України).

Цей підхід позбавляє громадян та організації впевненості в прийдешньому дні, що в результаті заважає вирішувати проблеми. Необхідно чітко визначити частку і межі державної участі в забезпеченні інформаційної безпеки, серед іншого шляхом законодавчого встановлення заборон та обмежень в розглядуваній сфері.

3.3. Поточний стан і тенденції розвитку державної інформаційної політики в Україні

Будь-якій демократичній державі об’єктивно необхідно реалізовувати власну інформаційну політику, оскільки максимальна відкритість для громадян − це один із принципів демократії. При цьому особлива відповідальність за це лежить на органах державної влади тих держав, які таку політику реалізують.

Держава посідає центральне місце у політичній системі, яка. В свою чергу, є сукупністю взаємодіючих одна з одною між ідей та норм, політичних

інститутів, що на них ґрунтуються, певних установ і дій, що організують політичну владу, а також взаємозв'язок між державою та її громадянами. Сам термін «політична система» увійшов у науковий обіг у середині XX століття (50−60-і роки). До того для опису владних відносин використовували поняття «система правління» або «тип правління», що зводило всю політику до діяльності державних структур і фактично до визнання цих структур головними суб'єктами владних відносин. Але світ не стояв на місці, тож, розвиток громадянського суспільства й визнання самостійної особи з її правами і свободами призвели до того, що громадянин став не лише підкорятися владним структурам, але і зі свого боку впливати на державу, засновуючи для цього відповідні політичні організації. У демократичних державах владні відносини набули більш складного характеру, оскільки у них почали брати участь і недержавні організації.

У політичний системі міститься кілька взаємопов'язаних між собою підсистем, що забезпечують функціонування публічної влади. За функціональною ознакою серед них можна виділити такі:

– інституційна підсистема − охоплює державу, громадські об'єднання (різні громадські організації, передусім політичні партії) та відносини між ними, з яких у сукупності і складається політична організація суспільства;

– комунікативна підсистема − містить у собі всі різновиди й форми політичної взаємодії як усередині системи певної держави, так і з політичними системами інших держав;

– нормативна підсистема − містить у собі політичні, правові та моральні норми і цінності, традиції, звичаї тощо;

– власне функціональна підсистема − охоплює способи здійснення влади й методи політичної діяльності.

Існує також і інша класифікація основних складових політичної системи:

– власне політична організація суспільства, що охоплює державу, політичні партії, інші громадські організації та об'єднання;

– політичні відносини − відносини, які складаються між різними підсистемами стосовно політичної влади;

– політична свідомість, що характеризує ідеологічні і психологічні боки політичної влади і політичної системи;

– політична практика, до якої, в свою чергу, належать політична діяльність і сукупний політичний досвід;

– соціально-політичні та правові норми, які врегульовують і регламентують політичне життя суспільства, а також реалізацію політичної влади.

Помітно, що кожен із зазначених варіантів як обов'язкову складову частину політичної системи суспільства містить інституційну підсистему. У контексті обраної теми дослідження саме вона викликає найбільший інтерес.

Підкреслимо, що загалом в усіх системах передбачається наявність структури й інституційної інфраструктури, на основі яких взаємодіють різні її складові. Більш того, структура в цьому випадку постає як основний компонент системи, що об'єднує навколо себе решту інших елементів цієї системи. Саму структуру політичної системи пропонуємо умовно вважати постійною величиною, зміна якої може потягти за собою серйозні наслідки, а складові системи правильніше розглядати як змінні величини. Природно, не варто забувати і про те, що політичні системи можуть бути дуже різними, і інститути, характерні для однієї з них, в інший можуть просто бути відсутні.

Ключовим, центральним елементом таких систем є держава, оскільки саме вона має монополію на законне насильство і передбачає «правила гри» для решти учасників такої системи. Це пояснюється тим, що конституція держави і взагалі все її чинне законодавство є обов'язковими для виконання всіма суб'єктами політичної системи відповідного суспільства. У самій же державі, у відповідності до функціонального поділу влади, діють виконавчі (уряд, міністерства, агентства, служби та ін.), законодавчі (парламент) і судові органи влади. Специфічну функцію тут виконує адміністративний апарат, який використовується владою для вирішення різноманітних завдань

у держав з різною політичною організацією – як у демократичних, так і в авторитарних. Так, часто під час передвиборчих кампаній лунають звинувачення з боку опозиції, що кандидатом, близьким до влади, був використаний так званий адміністративний ресурс, тобто допомога з боку місцевих чиновників.

Найактивніше у політичному житті суспільства беруть участь державні структури та держслужбовці цих структур. Наприклад, в усіх міністерствах у штаті є співробітників зі зв'язків з громадськістю, і вони можуть вести самостійну інформаційну політику. Нерідко трапляються випадки інформаційного суперництва або навіть інформаційних війн між окремими державними структурами. Щодо цього можна лише погодитися з думкою про необхідність урахування тієї обставини, що державна бюрократія є складовою політичної еліти і, як будь-елітна група, тому вона і переслідує власні політичні цілі, серед іншого і в інформаційній сфері. Положення вищих і частини середніх чиновників, що працюють у сфері виконавчої влади, об'єктивно надає їх посадам політичного масштабу, а також підвищує їх значимість у системі ухвалення державних рішень. При цьому державна бюрократія має перевагу перед конкурентним світом політиків, які обираються на певний строк, через те, що є більш згуртованим соціальним шаром, що володіє своєю корпоративною етикою і традиціями. Однак із суто політичної точки зору, бюрократія повинна залишатися політично нейтральною та ні при яких умовах не проявляти ангажованість тими чи іншими владними угрупованнями. Виконання чиновництвом суто адміністративних функцій, його невтручання у політичну боротьбу розглядається як одна з передумов збереження стабільності суспільних порядків. Звісно ж, наївно вважати, буцім чиновники обмежаться виконанням своїх чиновницьких обов'язків і не зв'язуватимуться з політикою або не намагатимуться впливати на ЗМІ. Як правильно було зауважено вище, чиновники не обираються народом, але вони зацікавлені у стабільності чинної команди. Найгостріше ця проблема стоїть в регіонах, де місцева

адміністрація намагається надати місце у парламенті якомога більшої кількості своїх прихильників, не гребуючи будь-якими засобами. Наприклад, якщо у регіоні є державні засоби масової інформації, то, звісно, місцеві державні службовці будуть намагатися впливати на їх інформаційну політику, особливо в період передвиборних кампаній. Нерідко буває, коли виконавча і судова влада діють узгоджено, і ці дії, як правило, спрямовуються проти незалежних засобів масової інформації або тих ЗМІ, що намагаються бути незалежними. Чиновники завжди прагнуть впливати на інформаційну політику різних ЗМІ, щоб створити собі позитивний образ в очах громадськості і бути популярними, інакше кажучи, в цьому питанні вони поводяться не як управлінці, а як публічні політики, і їх, так само, як і політиків, оточують політтехнологи та іміджмейкери. У демократичній державі діючий політичний режим не повинен втручатися в інформаційну політику ЗМІ незалежно від того, державні вони чи приватні [9; 72; 185].

Засоби масової інформації давно визнано дієвим інструментом впливу на соціальні відносини, можливості якого з розвитком інформаційних технологій дедалі сильніше зростають, через що цей інструмент дедалі активніше використовується тими, хто має фінансові ресурси та важелі адміністративного управління чи інші важелі впливу. Зазначена обставина актуалізує питання забезпечення державою інформаційної безпеки в суспільстві.

Деякі автори розуміють інформаційну безпеку як такий стан системи ЗМІ й характеру їх функціонування, коли всі соціальні суб’єкти (насамперед різні соціальні групи й окремі особи) незалежно від освіти, мови, місця проживання й інших чинників, а також різних об’єктивних і суб’єктивних перешкод, надійно отримують повну і достовірну інформацію, що оперативно надходить та забезпечує належний рівень інформованості, тобто надає всім без винятку соціальним суб’єктам можливість гранично всебічно і максимально об’єктивно відповідно до своїх потреб, положення в суспільстві орієнтуватися в дійсності та ухвалювати оціночні і поведінкові рішення,

адекватні ситуації, що склалася в конкретній сфері. При цьому обов'язком держави є забезпечення роботи стількох і таких каналів масової інформації і з такою різноманітністю, щоб це дозволило зробити відповідний потребам будь-якого згаданого суб'єкта вибір необхідних для забезпечення інформованості засобів масової інформації за умов забезпечення їх доступності, тобто, йдеться про максимальне полегшення отримання такими суб'єктами необхідної масової інформації [85; 87; 105; 117].

Інформаційна безпека в суспільстві залежить і від того, якою мірою кожен із соціальних суб'єктів у відповідності до своєї позиції і цілей має можливість поширювати від власного імені і в своїх інтересах масову інформацію, серед іншого створювати (засновувати або бути співзасновником) ЗМІ та мати для цього юридичні, економічні й інші можливості, щоб вільно знаходити, отримувати та компонувати інформацію. У такий спосіб забезпечується персональна інформаційна безпека і залучення потрібної аудиторію чи електорату [4; 124, с. 25–27].

На думку деяких науковців, не варто дивуватися боротьбі державних структур за право впливати на інформаційну політику державних засобів масової інформації. Ясна річ, що боротьба різних гілок влади за державні ЗМІ є природною. ЗМІ безпосередньо цікавлять державу і державні структури не як підприємства, що приносять прибуток (хоча врешті-решт усе зводиться саме до цього), а як інструмент впливу на громадськість. Боротьба між чиновниками точиться в першу чергу не за право контролювати фінансові потоки ЗМІ, а за контроль над інформаційною політикою. Чи може держава реалізовувати свою інформаційну політику, не вдаючись до допомоги ЗМІ? Звичайно, може, але для цього необхідно впроваджувати сучасніші інформаційні технології, перш за все Інтернет. Держава і державні структури можуть цілодобово інформувати населення про свою діяльність без допомоги посередників, якими виступають засоби масової інформації. Система, за якої громадяни і держава спілкуються безпосередньо, є

взаємовигідною, оскільки люди отримуватимуть інформацію у чистому вигляді без коментарів журналістів [39].

Населення цікавить, наприклад, яких успіхів досяг уряд у соціальній сфері, зокрема знизилося безробіття, збільшилися виплати на дітей тощо. Інакше кажучи, громадян цікавить статистика, яка не потребує коментарів, або, точніше, така, яку можна не коментувати, оскільки її дані говорять самі за себе. Звісно ж, уряд може спробувати приховати якісь негативні тенденції, що не дивно, або прикрасити свої досягнення в тій чи іншій галузі економіки, але за цим і повинна стежити преса. Якщо інформація на сайті уряду є достовірною і регулярно оновлюється, то цей інформаційний ресурс перетворюється на один із найголовніших каналів зв'язку між державою, її структурами та суспільством. Статистика, що складається на державній службі, містить значний обсяг інформації, тож, відповідно, обов'язком державної служби стає те, щоб зробити її доступною всьому суспільству. Вона має бути зрозумілою, і її треба забезпечити необхідними посиланнями на першоджерела. При цьому розповсюдження такої інформації, складеної урядом і для урядових потреб, не повинно обмежуватися міркуваннями секретності. І це поширення − не який-небудь додатковий обов'язок. Виконання цього завдання повинно стати одним із найвищих пріоритетів. Зараз, за допомогою сучасних інформаційних технологій, це завдання можна вирішити технічно й організаційно, і люди зможуть постійно бути в курсі того, що роблять, і над якими проблемами працюють органи державної влади, зокрема виконавчої. Різні групи користувачів не лише мають право на інформацію, зібрану і видану за громадський рахунок, ця інформація − важлива частина демократичного суспільства і гласної форми управління, відповідно, вся доступна інформація повинна широко розповсюджуватися.

Демократія передбачає повну відкритість для громадян, а органи влади в демократичній державі мають бути відкритими − це аксіома. Відповідно, прагнення до максимальної відкритості для громадян є природним, і фінансування програм щодо поліпшення інформаційної складової діяльності

державних структур має бути пріоритетним. Імовірно, це покращить їхню діяльність, оскільки людям не треба буде приходити до чиновників і питати, як заповнювати ту чи іншу форму, а громадяни легко зможуть ознайомитися з конкретною інформацією на сайті відповідної державної структури.

До найважливіших належить і проблема зниження корумпованості державних службовців, яка є актуальною не лише для України, але і для багатьох розвинутих країн, також схильних до корупції. Чим менше люди безпосередньо спілкуються з чиновниками, тим менше ймовірність того, що останні матимуть можливість вимагати гроші у прохачів, тому необхідно зробити мінімальну необхідність спілкування між адміністративними структурами та громадянами. Рішення проблеми корумпованості можливо у разі збільшення витрат на інформаційну політику державних інституцій і створення умов, за яких громадянин завжди знатиме, що і як йому робити без допомоги державного службовця, а за допомогою інформації, отриманої на сайті цієї організації.

Державне законодавство є чинним на території всієї країни, а якщо справа стосується регіонального законодавства, то можна вважати, що влада регіону або якогось іншого територіального утворення в змозі створити загальний інформаційний ресурс, який міститиме необхідну для громадян інформацію. Тому упровадження сучасних інформаційних і комунікаційних технологій та інформатизація держуправління на їх основі стає найважливішим моментом у створенні організаційно-технологічної бази реалізації державної інформаційної політики та її перебудови у відповідності до сучасних тенденцій розвитку розглядуваної сфери держави для:

– більш ефективного інформаційного обслуговування населення;

– покращення діяльності системи органів державної влади та місцевого самоврядування;

– формування, розвитку й використання загальнодержавної інформаційно-комунікаційної інфраструктури і системи інформаційних ресурсів.

Нагадаємо, що інформатизацію всіх сфер держуправління в цілому визнано одним із пріоритетних напрямів сучасної державної інформаційної політики.

Говорячи про вдосконалення роботи державних структур та інформатизацію держуправління, варто згадати і про комп'ютеризацію робочих місць держслужбовців та необхідність залучення фінансування програм із розвитку єдиних центрів обробки запитів громадян. Єдині центри обробки інформації є необхідними для того, щоб у державі накопичувалася статистика звернень населення з певних питань, і можна було ухвалювати рішення і робити висновки щодо того, які проблеми непокоять населення в першу чергу. Це дозволить виявити на ранній стадії ознаки невдоволення громадян та оперативно на них реагувати, не доводячи ситуацію до масових акцій протесту й інших активних дій, наприклад з вимогою відправити у відставку місцевих керівників [220].

Ефективним може бути лише той інформаційний центр, в якому інформація регулярно оновлюється, а обробка даних здійснюється в невпинному режимі. Не можна допустити того, щоб інформація застарівала, тобто інформаційні масиви слід утримувати в обновлюваному режимі й регулярно вносити до них зміни і доповнення, бо це прямо впливає на ефективність дії системи, адже, в кінцевому підсумку, і це стало вже аксіомою: інформаційна політика органу державної влади на загальнонаціональному або регіональному рівні повинна:

– мати попереджувальний характер;

– динамічно відображати реальні суспільні процеси;

– працювати на досягнення поставлених цілей;

– бути одним із важелів стратегічного управління держави.

Також державні органи можуть проводити моніторинг окремо взятої території чи всієї держави і з'ясовувати, що насправді хвилює населення, та з якими проблемами доводиться щодня стикатися громадянам.

Головними завданнями моніторингу є безперервне спостереження за станом соціально-економічної і фінансової сфери в регіонах та отримання про неї оперативної інформації. При цьому конче необхідним стає поточний аналіз на основі просторово-часової координації інформаційних потоків, які стосуються стану об'єктів моніторингу й формуються як органами виконавчої влади, так і іншими владними інституціями. Своєчасне виявлення змін у соціально-економічній та фінансовій сфері регіону та причин, які їх зумовили, попередження негативних тенденцій, що призводять до виникнення і подальшого зростання напруженості в соціально-економічній та фінансовій сферах, допоможуть стабілізувати становище. При цьому необхідно перелічити й інші необхідні для цього дії:

– короткострокове прогнозування динаміки найважливіших процесів у соціально-економічній і фінансовій сфері;

– оцінювання ефективності та повноти реалізації законів та інших нормативно-правових актів, присвячених соціально-економічним і фінансовим проблемам;

– оцінювання ефективності методів, організаційних структур і процесів управління стосовно органів державної влади і місцевого самоврядування, а також підприємств, організацій та установ усіх форм власності.

Регулярне здійснення моніторингу дозволить вирішувати проблеми на ранній стадії і, можливо, навіть зберігати стабільність в регіонах і на загальнодержавному рівні при оперативній реакції діючої влади як на місцях, так і у вищих органах влади. Державі і державним структурам краще дізнаватися про проблеми регіонів з допомогою моніторингу та ретельного аналізу одержаної інформації. Усі результати моніторингу мають бути опубліковані на сайті уряду і доступні для всіх бажаючих, тому що краще, щоб люди дізнавалися про проблеми від самого уряду, ніж з повідомлень преси [310].

Органи державної влади в демократичній державі не повинні боятися критики або осуду за їхні дії з боку громадськості, а після опублікування

результатів моніторингу їх представники зобов'язані пояснювати громадянам, що робиться для виправлення ситуації в проблемних галузях економіки або соціальної сфери. Необхідно працювати на випередження, не даючи ні опозиції, ні пресі приводів для критики діючої влади – цього можна досягти лише за умови грамотної внутрішньої інформаційної політики та наявності у штаті спеціалістів по зв'язках із громадськістю [362].

Існує стереотип, за яким органи державної влади постійно намагаються щось приховати, а журналісти хочуть донести до людей правду, але їм неодмінно хтось заважає, і тому у них (у журналістів), як і в опозиції, мало що виходить. Преса й опозиція користуються цим стереотипом і вдають із себе «інспекторів», які стоять на варті суспільних інтересів і стежать за діяльністю бюрократів.

З упровадженням новітніх інформаційних технологій виникає феномен максимальної відкритості державної інформації для громадян: «громадські виразки нашого часу» держава зможе «розкривати» самостійно і спілкуватися безпосередньо з громадянами.

Зрозуміло, що при цьому не йдеться про необхідність постійного звітування держави перед громадянами, а лише про те, щоб , як це передбачено принципами свободи слова і права на інформацію, забезпечити реалізацію передбаченого Конституцією права громадян на отримання інформації про діяльність державних органів влади. Так само зрозуміло і те, що ефективну реалізацію внутрішньої інформаційної політики держава зможе гарантувати лише за умови наявності технічних можливостей у населення отримувати потрібну інформацію, і тому завдання здешевлення і підвищення доступності інформації для громадян має стати першочерговим.

Діалог держави і суспільства повинен стати постійним, підґрунтям чого і слугує державна інформаційна політика. Діяльність різних державних органів у напрямі налагодження конструктивного діалогу з громадянським суспільством треба лише вітати і передбачати для цих цілей необхідну фінансову допомогу [237].

Залежно від того, на вирішення яких саме проблем – внутрішніх чи зовнішніх – цю політику націлено, можна виокремити такі її види:

– внутрішня політика − політика, яка має врегульовувати стосунки щодо головної соціальної (нею можуть виступати особа, мала або велика соціальна група, народ) або інституційної складової (держава і державні об'єднання, громадянське суспільство, громадські об'єднання тощо);

– зовнішня політика − політика, яка має врегульовувати стосунки суб'єкта, що її здійснює, з більш загальними або з іншими суб'єктами, включно, наприклад, з відносинами, з одного боку, між національною елітою і всією нацією, державою і її конкретними інститутами, а з іншого – між громадянським суспільством і його інститутами [8; 10; 88; 219].

Так, у тому разі, коли йдеться про вже сформоване громадянське суспільство, під яким розуміється високорозвинена людська спільнота, що є самокерованою системою, із власним суверенним правом на життєдіяльність, здатна здійснювати контроль над державою, то громадяни за таких умов обов'язково повинні мати можливість одержувати інформацію про діяльність владних та інших структур держави. Специфічними соціально-політичними рисами, які дозволяють відрізнити громадянське суспільство від догромадянського, є такі:

– вільна діяльність громадських об'єднань і соціальних інститутів – різноманітних асоціацій, громадських рухів тощо;

– гарантована реалізація усіх прав і свобод особи, реальне забезпечення її недоторканності та безпеки;

– наявність самостійності суб'єктів господарювання на тлі існування різних форм власності.

При цьому головними серед об'єднавчих принципів громадянського суспільства є самоврядування і справедливість [76; 104].

Держава, яка усвідомлює необхідність постійного власного розвитку, змушена активно займатися інформаційною політикою, а також свідомо формувати свої відносини з громадянським суспільством, перш за все з

політичними партіями, бізнесом та іншими головними акторами політичного процесу, адже згадана політика за своєю сутністю є насамперед діяльністю різних політичних сил щодо поширення інформації, покликаної забезпечити потреби держави і громадянського суспільства. Більш того, загалом висновок про ступінь демократизму суспільства можна робити саме на підставі взаємовідносин між державою та громадянським суспільством в особі громадських об'єднань (далі – ГО). Навіть сам факт створення недержавних об'єднань з ініціативи громадян яскраво відображає стан демократії та демократичних інститутів у цій державі. У цьому контексті також дуже важливим є правове закріплення взаємовідносин громадських об'єднань і держави. Громадяни та ГО завжди беруть активну участь в усіх політичних кампаніях, через що головним завдання держави в межах її інформаційної політики стає забезпечення плюралізму думок протягом таких кампаній та їх окремих заходів чи акцій.

Усе вищевикладене допомагає сформулювати визначення поняття «інформаційна політика держави». Зазначена політика є сукупністю цілей, які віддзеркалюють національні інтереси в інформаційній сфері, разом із стратегією, тактикою та завданнями держуправління в цій сфері, управлінськими рішеннями та методами їх втілення у життя, які державною влада формує і реалізує з метою регулювання і вдосконалення як процесів безпосередньо інформаційної взаємодії в суспільно-політичній та соціально-економічній сферах існування суспільства і держави, так і тих процесів, що уможливлюють цю взаємодію [8; 125; 177].

Відповідно до викладеного вище визначення, предметом інформаційної політики держави слід вважати:

– тенденції і закономірності розвитку інформаційної сфери, суспільних інформаційних відносин та інформаційних процесів, а також засоби й методи їх аналізу та прогнозування;

– дослідження впливу ЗМІ та засобів масової комунікації на свідомість мас, суспільство в цілому (зокрема, і громадянське) та державу разом із механізмами цього впливу.

Для глибшого аналізу інформаційної політики держави визначимо ті родові ознаки й форми, що їм відповідають, які стануть основою класифікації її конкретних проявів. На підставі цього можна виділити важливі для групування ознаки (підстави), перелічені нижче [7; 8; 125].

1. Суб'єктний зміст інформаційної політики держави – за цією підставою можна об'єднувати види й відповідні форми інформаційної політики залежно від її суб'єкта й, отже, від того, чиї інтереси відображатимуться у най найбільшою мірою:

– міжнародна інформаційна політика (рівень держав);

– партійна (пов'язана з лобіюванням);

– інформаційна політика спільнот (груп) різного рівня: національна, класова, елітарна тощо.

2. Часовий вимір розглядуваної політики − ознака, за якою види і відповідні форми цієї політики групуються залежно від тривалості політичного процесу, а також від завдань і цілей цієї політики, що вміщуються в певному часовому відрізку:

– колишня, сучасна і майбутня;

–тактична, стратегічна, довгострокова, короткострокова, оперативна тощо.

3. Територіально-просторовий вимір такої політики – ознака, за якою види і відповідні форми цієї політики об'єднуються залежно від території її поширення (чи просторової зони). За цією ознакою можна виокремити такі різновиди інформаційної політики:

− локальна;

− субрегіональна;

− регіональна;

− глобальна (її масштаби бувають як дійсно найширшими, якщо йдеться про глобальну політику в прямому сенсі цього слова, так і в разі потреби звуженими, наприклад до загальнонаціональної).

4. Спрямованість інформаційної політики держави щодо громадського прогресу − підстава групування видів, напрямів і відповідних форм цієї політики за ступенем (мірою) відповідності її змісту інтересам прогресу суспільства. За цією ознакою розрізняють реакційну, консервативну та прогресивну політики.

5. Методи провадження розглядуваної політики − підстава групування видів, напрямів і відповідних форм цієї політики за способами її реалізації. Зокрема, за цією ознакою і інформаційній сфері виокремлюються реформістська і радикалістська політика [8; 125; 237].

Реалізуючи інформаційну політику держави, учасники цього процесу можуть мати скільки завгодно різні цілі, тому завданням держави стає започаткування й налагодження конструктивного діалогу між ними, а також у цілому з громадянським суспільством, чому, як свідчить практика, може суттєво сприяти прозоре й об’єктивне інформування нею громадян про свою діяльність [234].

Інформація відіграє дедалі вагомішу роль в управлінні суспільством і всіма життєвими сферами. Водночас у процесі формування інформаційного суспільства відкритість інформації для громадян стає дедалі важливішою обставиною, а інформація, у свою чергу, перетворюється на неодмінний атрибут управління в цілому. За тим самим принципом інформаційне управління стає невід’ємною складовою інформаційного суспільства. Зауважимо, що в цьому разі йдеться про глобальне інформаційне суспільство, яке поступово охоплює всі країни світу, тобто про всезагальну інформатизацію, що об’єктивно починає вимагати належне й відповідне інформаційне забезпечення діяльності органів державної влади.

В інформаційній політиці держави можна виокремити дві головні складові – техніко-технологічну та гуманітарну. Перша із них стосується:

– вирішення завдань щодо подальшого перетворення суспільства на дійсно інформаційне;

– розроблення нових інформаційно-комунікаційних технологій і їх використання;

– створення відповідної конкурентоспроможної інфраструктури.

До гуманітарної складової розглядуваної політики держави належать зміст і якість інформації, використовувані в ній поняття, вплив цієї політики на політичні, соціальні та інші процеси в суспільстві тощо. Через це гуманітарну складову державної інформаційної політики доречно визнати визначальною (рис. 3.1) [8; 125; 266].

Рис. 3.1. Модель вдосконалення державної інформаційної політики
Джерело: авторська розробка

Суб'єкта, що провадить інформаційну політику в умовах глобалізації, має робити це, враховуючи, що в зоні його активності вона здатна актуалізувати не лише ті інтереси, що існують у геополітичному просторі перебування цього суб'єкта, але й ті, які зачіпають інтереси багатьох інших суб'єктів в усьому світу, що притаманно глобальності як такій. Саме через такий тісний зв'язок з динамікою глобалізації інформація ввійшла до переліку ключових напрямів технічного прогресу, серед іншого у сфері держуправління та його інформаційного забезпечення.

Умовно методи аналізу державної інформаційної політики зручно об'єднати у дві основні групи. Першу з них складають методи, що стосуються дослідження чи пізнання взагалі всіх політичних явищ і процесів, зокрема і розглядуваної політики. Фактично − це методи політології як науки, що використовуються в цьому випадку для аналізу конкретного політичного процесу. Друга група охоплює сукупність специфічних методів реалізації інформаційної політики держави. Зрозуміло, що кожна з цих груп має цілком самостійне значення, оскільки використовується для дослідження різних аспектів цієї політики [8; 266].

Щодо характеристики першої групи методів зауважимо, що їх, у свою чергу, можна поділити ще на кілька підгруп. Найважливішими серед останніх є методи оцінювання та подання інформації, відмінною рисою яких виступає орієнтація на специфічну інтерпретацію державної інформаційної політики та її проявів і, відповідно, − на особливий підхід до її аналізу.

До таких методів слід віднести:

1) антропологічний − орієнтується на оцінювання й аналіз державної інформаційної політики держави як явища, зумовленого природою людини (як родової істоти);

2) соціологічний − орієнтується на оцінку й аналіз розглядуваної політики як явища соціально обумовленого економікою, соціальною структурою, ідеологією і культурою;

3) психологічний − орієнтується на оцінку й аналіз цієї політики як явища, обумовленого психологічними характеристиками людей, включно з їхніми соціально-психологічними особливостями;

4) біхевіористський − орієнтується на оцінювання й аналіз такої політики як явища, що істотно впливає на поведінку окремих осіб і груп;

5) нормативно-ціннісний − орієнтується на оцінювання й аналіз державної інформаційної політики з точки зору її аксіологічної сутності, відповідності функціонуючим та ідеальним нормам і цінностям;

6) процесуальний − орієнтується на її оцінювання й аналіз як циклічного процесу, що має певні фази або стадії;

7) структурно-функціональний − орієнтується на її оцінювання й аналіз як явища, що володіє складною структурою, кожний елемент якої має певне призначення і виконує свої специфічні функції;

8) системний − орієнтується на її оцінювання й аналіз як цілісного, впорядкованого і саморегульованого механізму;

9) інституційний − орієнтується на оцінювання й аналіз тих соціально-політичних інститутів, за допомогою яких реалізується державна інформаційна політика;

10) критично-діалектичний − орієнтується на оцінювання й аналіз інформаційної політики держави з погляду її критичного розгляду, а також щодо виявлення суперечностей як джерела її саморуху;

11) порівняльний − орієнтується на оцінювання й аналіз розглядуваної інформаційної політики шляхом зіставлення її однотипних форм, що функціонують в різних умовах, з метою їх оптимізації;

12) історичний − орієнтується на оцінювання й аналіз цієї політики з огляду на її послідовний часовий розвиток, на виявлення в ній зв'язку минулого, теперішнього і майбутнього [8; 125; 266; 365].

Іншу підгрупу першої групи становлять методи організації та процедури дослідження інформаційно-пізнавального процесу. І хоча методи цієї підгрупи не мають специфічного політологічного характеру і можуть використовуватися усіма іншими науками, вони, тим не менше, мають важливе значення у справі підвищення ефективності вивчення розглянутого процесу.

До цієї ж підгрупи належать такі головні методи:

– аналіз і синтез;

– індукція та дедукція;

– абстрагування;

– рух від абстрактного до конкретного;

– об'єднання історичного і логічного аналізу;

– аналогія;

– моделювання [7; 163].

Окрему підгрупу, яку можна виділити всередині першої групи, складають також методи отримання первинної (необробленої) інформації про пов'язані з політикою явища, події та факти. До них належать перелічені нижче методи.

1. Метод спостереження − серед методів отримання первинної інформації використовується частіше за все. При цьому спостереження може бути короткочасним, середнім за терміном часу і довготривалим,

індивідуальним і колективним, безпосереднім (коли спостерігач безпосередньо бере участь у політичних подіях, що ним досліджуються), і стороннім (тобто зовнішнім).

2. Опитування − найважливіший інструмент дослідження громадської думки. У практиці воно застосовується фактично як метод політичної розвідки і виявлення поглядів населення на різноманітні проблеми, пов'язані з політикою. З часом вони перетворилися з методів виявлення настроїв громадян на засіб надання певної спрямованості цим настроям. Виступаючи інструментом пропаганди й одночасно виконуючи допоміжну роль відносно ЗМІ, такі опитування дають змогу перевірити ефективність пропагандистського забезпечення певного політичного курсу. Нерідко опитування громадської думки використовуються для свого роду програмування і можуть бути використані для маніпулювання цією думкою [8; 47; 166]. Тоді ЗМІ перетворюються на знаряддя, які допомагають несумлінним учасникам політичної гри реалізовувати свої задуми.

Розрізняють такі форми опитування:

– анкетне опитування − вид опитування, за допомогою якого на базі вибіркового статистичного аналізу визначається думка конкретних груп людей (аж до громадської думки) про певні політичні події, явища тощо, а також подається наукова інтерпретація отриманих формальних даних для розроблення відповідної лінії політичної поведінки або її коригування;

– інтерв'ю − опитування, що проводиться, як правило, за заздалегідь наміченим планом і темою, під час якого відбувається прямий контакт інтерв'юера з учасниками політичних подій.

3. Бесіда відрізняється від інтерв'ю тим, що має двосторонній характер, внаслідок чого її учасники перебувають в рівному становищі.

4. Аналіз статистичних матеріалів − метод, що дозволяє абстрагуватися від обмежень часу і простору і на підставі завантажених статистичних відомостей виявити відповідні тенденції або простежити діючі закономірності.

5. Вивчення документів. Цей метод охоплює аналіз офіційних матеріалів (стенограм засідань уряду або парламенту, документів політичних партій, різних програм тощо), особистих документів (листи, щоденники, мемуари), а також фото-, аудіо-, кіно -, відеодокументів тощо).

6. Експеримент − метод, у разі застосування якого імітується розвиток того чи іншого політичного явища, завдяки чому стає можна передбачати подальший перебіг реального політичного процесу як результат розкриття його внутрішніх механізмів [1; 311].

Не применшуючи значення першої групи методів, слід підкреслити, однак, що найбільш ефективною виступає група специфічних методів реалізації інформаційної політики.

Існує ціла низка напрямів забезпечення державою своєї інформаційної політики. Найважливіші з них − фінансово-економічний, організаційно-технічний і правовий.

Зокрема, фінансово-економічні методи передбачають:

– удосконалення системи фінансування робіт з розроблення програм для забезпечення інформаційної безпеки;

– формування системи страхування інформаційних ризиків для фізичних та юридичних осіб.

Організаційно-технічні методи, відповідно, передбачають:

– створення і використання засобів захисту від несанкціонованого доступу до оброблюваної інформації;

– розроблення програм, які перешкоджають руйнуванню та викривленню інформації;

– покращення якості професійної та спеціальної підготовки користувачів інформаційних систем;

– постійне спостереження за діями обслуговуючого персоналу в захищених інформаційних системах.

Правова або законодавча діяльність держави із забезпечення інформаційної безпеки охоплює такі заходи.

1. Розроблення законів та інших нормативно-правових актів, де передбачається відповідальність фізичних і юридичних осіб за:

– несанкціонований доступ до інформації;

– розголошення інформації, що містить державну або комерційну таємницю;

– викривлення, протизаконне використання або протиправне копіювання інформації;

– використання в злочинних цілях службової інформації;

– навмисне розповсюдження недостовірної інформації.

2. Створення нормативно-правових актів, що обмежують частку іноземної участі у володінні загальнодержавними ЗМІ.

3. Установлення законодавчого розмежування повноважень у галузі інформаційної безпеки між органами влади.

4. Розроблення нормативно-правових актів щодо регламентації взаємовідносини держави з контрагентами (як поза межами держави, так і всередині неї) в інформаційній сфері.

Найважливіше місце у системі інформаційних загроз для суспільства посідають такі:

– посилення психоемоційної напруженості в суспільстві, її нагнітання аж до руйнування психіки;

– масове використання технік маніпулювання та дезінформації, здатне заподіяти шкоду інтересам громадян;

– підміна культурних цінностей, що сформувалися, усталеної морально-етичної системи стандартів або релігійних вірувань;

– монополізація інформаційної сфери суспільства.

Інтернет − один з видів комунікацій, що найбільш динамічно розвиваються. Його основна перевага − оперативність, швидкість доставки інформації від творця до споживача. Перехоплювати або контролювати інформаційні потоки в Інтернеті досить проблематично, і пов’язано це, перш за все, з великими масивами інформації, які постійно циркулюють у

кіберпросторі. Досить вражаючими виглядають темпи розвитку і поширення Інтернету в світі. Якщо, наприклад, телефону, щоб зайняти 30 % ринку домашніх господарств, знадобилося 38 років, то Інтернету − всього 7. Цю тенденцію можна описати і таким чином: щоб охопити аудиторію в 50 млн осіб, радіо знадобилося 38 років, персональному комп'ютеру − 16, телебаченню − 13, а Інтернету − 4 роки. Інтернет перетворився на арену політичних баталій, і тому політичним акторам необхідно приділяти серйозну увагу викладенню й обґрунтуванню своїх поглядів і цілей в Інтернеті. Державі, що прагне до відкритості та окремим державним структурам бажано, зокрема, мати персональну сторінку в глобальній мережі, дозволяючи усім бажаючим громадянам будь-коли мати доступ до будь-якої інформації про діяльність відповідної державної служби. Втім, у цьому контексті не важливо не забувати і про мережеву безпеку, оскільки в інформаційних війнах часто використовується саме Інтернет, простір якого ніким не контролюється [75; 156; 174; 185].

Інформаційна війна є найпоширенішим типом інформаційних кампаній. Цікаво, що відразу декілька інформаційних кампаній можуть проводитися одночасно різними політичними силами, не вступаючи в заочну полеміку між собою. Такий варіант проведення інформаційних кампаній можна назвати цивілізованим. У зазначеному вище випадку йдеться про інформаційне суперництво, а не про інформаційну війну: чия позиція здаватиметься суспільству більш правильною і конструктивною, того люди і підтримають [55; 57; 62; 68; 74; 75; 156; 172, 173; 174; 185; 243].

Інформаційна кампанія являє собою цілий комплекс заздалегідь спланованих і взаємопов'язаних дій, які спеціально розробляються для досягнення конкретних цілей комунікатора і передбачають цілеспрямований вплив на громадську думку та позиції контрагента. Інформаційна кампанія завжди має конкретну мету і передбачає цілеспрямований вплив на громадську думку. Зазвичай, інформаційні кампанії запускаються перед

виборами або референдумом та розповсюджуються зацікавленими особами, серед іншого державою [185].

При цьому необхідно розглянути етапи розгортання інформаційної кампанії. Існує кілька моделей проведення інформаційних кампаній, але найчастіше використовується триступенева модель. На першій ступені вирішуються суто організаційні питання, а саме складання і затвердження кошторису (бюджету) планованих заходів (адже, якщо це загальнонаціональна інформаційна кампанія, із залученням телебачення та впливових друкованих видань, то для її проведення потрібні серйозні вкладення). Друга стадія вже передбачає початок активних дій: наприклад, на сайті одного впливового інформаційного агентства з'являється заздалегідь підготовлена інформація, яку тут же підхоплюють (природно, невипадково) інші ЗМІ. На останній, третій стадії вже доводиться відбивати і можливі контратаки опонентів. Тут треба ще зважати на те, що політичні опоненти можуть оперативно відреагувати на опубліковану в пресі інформацію і контратакувати настільки успішно, що вся кампанія може виявитися провальною [185].

Іноді інформаційні кампанії влаштовують безпосередньо для отримання прибутку. ЗМІ не відрізняються об'єктивністю під час інформаційних кампаній і активно беруть участь у них, видаючи своїм глядачам, слухачам і читачам ангажовану інформацію. Опозиційні ЗМІ часто поширюють неправдиву інформацію про опонентів або органи державної влади, тобто дезінформацію. Маніпулюючи громадською думкою через підконтрольні ЗМІ, опозиція набирає політичні бали. У такий спосіб політики (як провладні, так і опозиційні) позбавляють людей права на об'єктивну, незаангажовану інформацію [73; 85; 135; 136; 139; 174].

Існують ще незалежні ЗМІ, але насправді вони є дуже залежними від своїх власників, які мають ті чи інші політичні погляди. Інакше кажучи, державна внутрішня інформаційна політика також не є гарантією об'єктивності. Така політика може обслуговувати державу і не задовольняти

інтереси громадянського суспільства, вступати в діалог з державою або виступати проти нього, або обстоювати виключно інтереси окремих груп, угруповань, партій і навіть окремих осіб [73; 135].

Якщо, наприклад, власник інформаційного агентства спеціалізується виключно на обслуговування інтересів однієї політичної партії, чиї погляди він поділяє, то в цьому немає нічого кримінального, оскільки інформагентство − його власність, і він вправі з допомогою свого агентства підтримувати тільки ту або іншу партію, і це співробітництво найчастіше взаємовигідно. Дружні ЗМІ можуть розраховувати на ексклюзивні інтерв'ю та заплановані витоки інформації з обізнаних джерел, а інформація − це основний продукт інформагентства, відповідно, власникові агентства така взаємодія є вигідною і навіть прибутковою.

У цілому інформаційна війна − це здійснюване в інформаційні способи протистояння між державами в інформаційному просторі, в якому для дестабілізації суспільства і державних структур супротивника передбачається заподіяння шкоди інформаційним системам, процесам і ресурсам критично важливих структур з метою підриву політичної, економічної і соціальної систем, а також масова психологічна обробка населення [42; 52; 55; 57; 68; 142; 156; 174; 185; 243].

Ведення сучасних бойових дій передбачає використання інформаційних комунікацій для заподіяння інформаційно-психологічного збитку супротивникові. Природно, що описаний вище вид інформаційного протистояння може реалізовуватися лише в межах зовнішньої інформаційної політики, оскільки жодна держава не зацікавлена в дестабілізації всередині власної країни, за винятком різних радикалів, які закликають до насильницького повалення влади і повної зміни політичної й економічної систем, однак ті зазвичай не мають доступу до масових комунікацій для здійснення масштабних інформаційних воєн, і тому не є надто небезпечними.

Існує і інший спосіб ведення інформаційних війн, він може спостерігатися як між державами, так і між конфліктуючими політичними

акторами всередині країни. Цей вид протистояння не передбачає використання військової сили, скоріше це спроба уникнути військового зіткнення. Ця ситуація виникає, коли різні суперечності на міждержавному рівні намагаються вирішити за допомогою інформаційної переваги над інформаційними системами противника і нав'язування власних поглядів на ті чи інші проблеми, серед іншого діючи всередині держави-жертви за допомогою агентів впливу. Держава-агресор за допомогою підкуплених або куплених ЗМІ, ГО і навіть відомих політичних діячів здійснює свою інформаційну політику і в такий спосіб намагається «перетягнути» громадську думку держави-жертви на свій бік [68; 72; 135; 139; 142; 243].

Держава не повинна поводитись пасивно в період інформаційної війни, їй треба мінімізувати збиток від інформаційної атаки противника, використовуючи контратаки і власні системи комунікацій для контрпропаганди. Для цього в своїй внутрішній інформаційній політиці державі необхідно спростовувати пропаганду противника й оперативно реагувати на всі зловмисні інформаційні повідомлення, не даючи можливості ворожій інформації досягти своєї мети. Державі слід прагнути до консолідації всього суспільства, і тому для реалізації цілеспрямованої внутрішньої інформаційної політики їй доводиться використовувати всі наявні й можливі інформаційні канали комунікації [68; 171; 185; 243].

За своєю суттю політична пропаганда є особливою формою інформаційних потоків, що стосуються політики і влади. Для неї є характерними такі ознаки: односторонність, монологічний спосіб подання, формування не враховуючи думок реципієнта, на основі вкрай критичного ставлення того, хто займається пропагандою (комунікатора) до всього, що стосується його конкурентів, насамперед до їх поглядів і позицій [9].

За іншим формулюванням, у політичній пропаганді завжди присутнє ігнорування з боку комунікатора потреби інших людей в достовірній інформації, яке може бути як відкритим, так і зовні непомітним, а головне – штучне насаджування його власних поглядів, ідей, ідеалів тощо, що робиться

для того, щоб вплинути на громадську думку і змінити її у бажаному (вигідному) для комунікатора напрямі, щонайменше підказка суспільство, як воно повинно має. Оскільки за таких умов люди (населення певної території, усі громадськість певної держави чи якась її частина) фактично виступають лише мішенню, пропаганда вважається саме одностороннім процесом [85].

Існує дуже багато різних видів пропаганди. Найчастіше в науковій літературі виокремлюють такі її основні різновиди:

– офіційна пропаганда − головною її відмінністю є її, так би мовити, офіційний характер, її може здійснювати лише суб'єкт інформаційної політики (держава, правляча партія тощо); зазвичай для неї застосовуються особливі інформаційні технології, зумовлені згаданою обставиною;

– неофіційна пропаганда − на відміну від першої, ґрунтується на застосуванні технологій, за якої суб'єкт інформаційної політики для досягнення своїх цілей на політичному ринку формулює свої завдання і мету негласно, певною мірою конфіденційно (що і зумовлює її особливий характер);

– позитивна пропаганда − вважається такою, якщо ідеї, які вона просуває, за змістом виявляються для певного суспільства позитивними і конструктивними;

– негативна пропаганда − просуває ідеї, які завідомо можуть виявитися шкідливими для певних верств населення; вона часто відрізняється упередженістю;

– «чорна» пропаганда − ґрунтується на безпосередньому застосуванні фальсифікації та дезінформації і здійснюється за допомогою таких технологій і методик, що суперечить морально-етичним і нерідко правовим нормами відповідного суспільства;

– «біла» пропаганда − здійснюється з оголошенням актора та джерел походження інформації з використанням законних і всім відомих форм поширення;

– «сіра» пропаганда − відрізняється тим, що джерела інформації в ній приховуються, лишаються анонімними, а також застосуванням таких інформаційних технологій, які перебувають на межі допустимого, дозволеного громадською мораллю, і вважаються в цьому суспільстві не зовсім гідними;

– пряма пропаганда − така форма, в якій заклики, заяви, висловлювання, критика на опонентів тощо є відкритими і публічними;

– непряма пропаганда − впливає на реципієнтів завдяки наявності прихованих натяків, різних підтекстів і подібних до цього технологій;

– пропаганда засобами мистецтва − відрізняється тим, що діє опосередковано, формуючи у реципієнтів за допомогою художніх засобів літератури, музики, архітектури, живопису тощо бажану для комунікатора систему суб'єктивних уподобань і схильностей, за допомогою чого людей схиляють до прийняття тих чи інших ідей, ідеологій, доктрин, цілей тощо;

– наукова пропаганда − реципієнтів переконують, спираючись на ті або інші наукові концепції і доктрини, висновки з яких за змістом є вигідними для комунікатора;

– ідейна пропаганда − головною метою і сутністю є поширення тих або інших масштабних «національних ідей», систем цінностей або спільних для відповідного соціуму цілей, спрямованих на інтеграцію певних політичних груп, кіл, спільнот і груп чи цього суспільства в цілому;

– пропаганда дією − спирається насамперед на залякування реципієнта, зазвичай апелюючи до болючих для певної аудиторії тем, як-то фінансова криза, теракти, стихійні лиха, ризик програти війну тощо;

– ретиальна пропаганда − відрізняється масовістю об'єкта, націлена на широку аудиторію, для цього використовуються особливі структури та/або механізмів поширення інформації від ЗМІ до спеціальних відомств;

– аксіальна пропаганда − націлена на певну вузьку частину населення (спеціальну цільову аудиторію);

– соціологічна пропаганда − відрізняється задіюванням певних елементів буденного для реципієнтів предметного середовища, завдяки чому прищеплюванні нею ідеологічні чи політичні уподобання людей нерідко виявляються не усвідомленими [9; 85; 281].

Варто підкреслити, що ці форми і технології зазвичай не залежать від конкретного змісту ідей, які просуває така пропаганда, і можуть використовуватися будь-якими сторонам. Так, наприклад, немає жодних принципових відмінностей між пропагандистськими технологіями, які в період «холодної війни» застосовували СРСР і США. Фактично те ж саме відбувається і в XXI столітті, вдосконалюватися продовжують головним чином лише системи комунікацій (Інтернет, соцмережі тощо).

Важливе значення для аналізу пропаганди має розуміння її функцій. Історично вони також майже не змінювалися. Найголовніші з них перелічено нижче.

1. Боротьба з ідейними супротивниками – у цьому разі структура і зміст пропагандистського впливу покликані дискредитувати політичні погляди, ідеї та/або програми опонентів і завдяки цьому зробити їх менш популярними.

2. Управління інтерпретаціями подій, в разі якого реципієнта переконують у правомірності поглядів і позицій суб’єкта пропаганди. Пропаганда цього штибу не стільки намагається донести до масової аудиторії якусь інформацію, скільки намагається змінити саме сприйняття реципієнта таким чином, щоб той заздалегідь віддавав перевагу думкам та оцінкам комунікатора. Так, вона прагне нав’язати аудиторії конкретні логічні схеми оцінювання та розуміння подій, певні зразки мислення, і за допомогою такої уніфікації політичного мислення може досягти ідеологічного контролю над громадською думкою. Фактично пропаганда у публічній політиці виступає інструментом політичних постатей, які намагаються монополізувати інформацію про їх інтереси і цілі.

3. Обов'язкова відповідь на закиди політичного опонента, нейтралізація його зусиль – те, що найчастіше позначають терміном «контрпропаганда». Вважається однією з найважливіших функцій пропаганди. Практика свідчить, що вдале і своєчасне реагування на інформаційні напади з боку політичних конкурентів здатне «обнулити» результат будь-яких інших його пропагандистських зусиль.

4. Контроль над свідомістю населення, використовується як для «вербування» нових прихильників тих чи інших ідей і цілей, так і для утримання їх у підлеглому, залежному стані. Саме ця функція перетворює пропаганду на певний інструмент як загального, так і власне політичного контролю.

5. Практична активізація свідомості, за якої відбувається переведення знань та уявлень комунікатора у галузь поведінкової мотивації реципієнта [9; 19; 72; 281].

Серед способів інформування найбільш характерним для пропаганди є маніпулювання.

Маніпулювання як форма впливу, будучи особливим методом інформування, передбачає ставлення комунікатора до реципієнта як до засобу для досягнення своїх цілей і прагнення до отримання одностороннього виграшу, відповідно, воно характеризується прихованими способами впливу і використанням різноманітних слабкостей опонента [131].

Система маніпулювання побудована таким чином, щоб оцінки комунікатора пригнічували оцінки і судження реципієнта. Маніпулювання одночасно передбачає і використання інструментів, які зовні маскують застосування цієї моделі до мислення реципієнта інформаційної технології, а також змінюють до невпізнання його істинні смисли і задуми. Технологія маніпулювання спрямована, насамперед, на суспільні маси, не надто обізнані в політичних або макроекономічних питаннях. Комунікатор інтерпретує події у вигідному для себе контексті, намагаючись при цьому уникнути дискусії з висококваліфікованими опонентами. Маніпулювання передбачає

застосування дезінформації, наприклад для поширення неправдивої інформації або приховування будь-яких невигідних комунікатору даних. Основною політичною метою дезінформації є провокування опонента на непідготовлені дії або бажання спрямувати його дії у хибному напрямі [9; 85].

Поряд із пропагандою в реалізації інформаційної політики активно й досить таки ефективно використовується агітація. Як і пропаганду, її спрямовано на управління свідомістю реципієнта, але агітація має кілька відмінних від пропагандистських технологій особливостей, що дозволяє розглядати її окремо. Якщо пропаганда створює і поширює якісь розумові схеми, то агітація намагається стимулювати поведінкову активність людей, прагнучи застосувати певні культурні зразки їх поведінки і взаємодії у сфері політики. Агітація формується з функціонального призначення і переваги. Такою є, наприклад, агітація в підтримку реформ або лінії партії [9].

Розрізняють кілька способів організації інформаційних потоків − маркетингові і немаркетингові. Розглянуті вище способи мають немаркетинговый характер (пропаганда, агітація). Маркетинг − це, скоріше, управління просуванням інформації, а не спосіб маніпулювання суспільною свідомістю. Реципієнт отримує інформацію, яка відповідає його потребам та уподобанням. Маркетинг передбачає інформаційний обмін, тобто інформаційна політика ведеться таким чином, щоб постачати інформаційний продукт з урахуванням потреб і бажань реципієнта [19; 144; 164]. Маркетинговий спосіб реалізації інформаційної політики застосовується у таких формах:

– політичного піару;

– інформаційного лобізму;

– політичної реклами;

– інформаційного тероризму.

Інакше кажучи, маркетинг потрапив у політику з бізнесу, де він активно використовується для реалізації, тобто продажу, різної продукції. У

разі такого підходу політик чи політичні ідеї перетворюються на продукт, який маркетолог повинен подати споживачу (населенню)у вигідному вигляді. Найбільшого поширення маркетингові технології набули в США, де фахівці з PR формують відповідний образ політика та починають його розповсюджувати.

У маркетинговій стратегії на перше місце виходить ретельне планування виступів кандидата і взагалі його появ на публіці. Усі ці дії називаються політичним іміджмейкінгом і є майже невід'ємною складовою маркетингових технологій. Імідж − це образ політика, який створюється штучно і може далеко відходити від його реальних якостей і характеристик. Для фахівця зі створення публічного образу головне − сформувати привабливий для споживача образ, який може користуватися популярністю на виборах і підтримкою населення в цілому. Однією з найпоширеніших форм маркетингового способу інформування є технологія політичного піару. Це особливий різновид маркетингової інформаційної діяльності, покликаної створювати позитивний імідж і відповідні комунікації об'єкта для реалізації конкретної мети, а також допомагає підтримувати стійку, довготривалу атмосферу, яка забезпечує довірче ставлення партнерів і контрагентів до його активності в політичній сфері [144; 164].

Продовжуючи аналіз технологій політичного піару, необхідно підкреслити, що існують деякі відмінності між піар-комунікацією і піар-діяльністю. Так, піар-комунікація спрямована, насамперед, на створення конструктивних відносин із суспільством − вона є різновидом альтруїстичного способу, тобто не спрямована на негайне отримання вигоди. У підґрунті піар-діяльності лежить прагматичний інтерес замовників, які прагнуть вплинути на громадську думку або навіть управляти нею [132].

Застосування піар-технологій передбачає використання ряду основоположних принципів. Зокрема, необхідно:

– постійно коригувати позиції, спираючись на маневреність поведінки акторів, їх здатність адаптуватися до будь-якої ситуації;

– прагнути до забезпечення взаємної вигоди інформаційних партнерів;

– не виключати можливість самокритики;

– намагатися мінімізувати застосування ідеологічних положень;

– намагатися переконати споживача інформації замість його схилення до визначеної моделі поведінки;

– підтримувати відкритий характер інформаційних відносин;

– спиратися на громадську думку [164].

Крім піар-технологій, маркетингова стратегія передбачає використання інформаційного лобізму як способу інформаційного супроводу.

Інформаційний лобізм є способом формування і підтримки комунікацій із власними, специфічними нормами та принципами обміну інформацією і відтворення політичних контактів, каналами спілкування й іншими структурними компонентами.

Інформаційний лобізм спрямований, насамперед, на встановлення двосторонніх відносин і утворення зворотних зв'язків комунікатора з реципієнтом. Цей процес має локально-точковий характер, і головною метою лобіста є особа чи група осіб, які впливають на ухвалення потрібних лобісту рішень. Як і інші маркетингові технології, інформаційний лобізм вибудовується з урахуванням позицій і потреб реципієнта [144].

У разі застосування методу інформаційного лобізму контакти з посадовими особами мають не публічний характер і не є головною метою, оскільки виступають в цьому випадку всього лише інструментом реалізації розглянутого виду маркетингової технології. Цей вид комунікації має досить короткостроковий характер через те, що після ухвалення потрібного лобісту рішення встановлена комунікація втрачає свою значимість.

Серед типів інформаційного лобізму виділяють такі.

1. Внутрішній тип − зацікавлені в ухваленні рішення особи встановлюють контакти з потрібними чиновниками, будучи при цьому частиною тієї ж системи, тобто вони лобіюють потрібне їм рішення всередині відомства, в якому самі працюють.

2. Зовнішній тип − найпоширеніший тип інформаційного лобізму. Тут комунікатори проникають у зону ухвалення рішень, перебуваючи при цьому поза системою. З легальних способів цього типу інформаційного лобізму можна виділити надання посадовій особі вигідної комунікатору інформації.

3.Загальнонаціональний тип − вибудовується з урахуванням специфіки країни і політичного режиму.

4. Непрямий тип − комунікатор бере собі в союзники громадську думку і, спираючись на дані соціологічних опитувань, чинить тиск лобіста на особу, яка приймає рішення з певного питання.

Також, як уже згадувалося вище, важливою формою маркетингового способу інформування виступає політична реклама.

Узагалі, як відомо, реклама використовується для просування різних товарів на ринку. Точно так само політична реклама існує для просування політичних товарів на політичному ринку. При цьому політичним продуктом, який реалізують за допомогою реклами, можуть бути як окремі політики, так і політичні об’єднання, що зацікавлені у власній популяризації серед населення [144].

Неодмінною об’єктивною умовою існування і розвитку політичної реклами є функціонування багатопартійної системи, оскільки саме наявність конкурентів змушує соціальних й інституційних політичних акторів та їхніх лідерів звертатися за допомогою до піар-фахівців і маркетологів, щоб популяризувати свої погляди серед електорату [9].

Виділяється кілька видів рекламних дій, які сприяють просуванню рекламного продукту на політичному ринку. Основними серед них є такі.

1. Рекламні дії, спрямовані на формування активного попиту на пропонований політичний товар. Зазвичай такі дії стають успішними за рахунок організації цільових звернень до споживачів, здатних стимулювати їх реакцію на політичну продукцію.

2. Рекламні дії, що сприяють продажу, під час проведення яких акцент робиться не на сам товар, а на чинники, супутні його просуванню, − додаткова інформація про політичний продукт.

3. Рекламні дії, що сприяють проникненню товару на політичний ринок, його виділенню серед конкурентних і закріпленню в цьому просторі. Їх здійснення націлене на виявлення і подачу споживачеві специфічних властивостей і якостей пропонованого продукту, відмінних від тих, які рекомендують політичні конкуренти.

4. Рекламні дії, які сприяють просуванню товару на політичному ринку за рахунок обігравання суперника і, як наслідок − посилення стимуляції збуту.

5. Рекламні дії щодо популяризації, що співвідносяться з конкретними суб'єктами політики ідеологій, програмними завданнями, політичними принципами тощо [132].

Під час виробництва рекламної продукції перед її творцями і розповсюджувачами стоїть низку завдань, які поділяються на:

– соціально-економічні;

– соціально-психологічні;

– організаційні;

– аналітичні.

Зокрема, соціально-економічні завдання вирішуються за допомогою визначення:

– витрат на експертизу політичної кампанії чи окремої акції;

– фінансових джерел рекламних акцій;

– коштів на виробництво відмінної від інших рекламної лінії (плакатів, сувенірів тощо);

– фінансових витрат на вибір носіїв і засобів доставки рекламної продукції споживачеві.

Соціально-психологічні завдання спрямовані на те, щоб вступити в емоційно-чуттєвий контакт зі споживачем рекламної продукції. Для

вирішення соціально-психологічних завдань особливого значення набуває грамотно підібраний рекламний текст, що враховує проблеми і запити цього контингенту. Виробнику реклами необхідно увійти в психологічний контакт зі споживачем і привернути його увагу.

Організаційні завдання вирішуються шляхом узгодження різних акцій, наприклад виступ політика по радіо і по телебаченню має бути в різний час з метою збільшення потенційної аудиторії. Завдання такого роду вирішуються шляхом планування рекламних заходів.

І, нарешті, аналітичні завдання вирішуються за допомогою:

– дослідження політичного ринку;

– визначення основних гасел майбутньої рекламної кампанії;

– виділення адресних груп, на які вона спрямована.

По закінченні рекламної кампанії визначається ефективність обраної стратегії і рекламних дій, що реалізовувалися протягом неї.

Специфічною формою маркетингового способу інформування виступає інформаційний тероризм, спрямований на нанесення реципієнту шкоди, насамперед психологічної. Як правило, інформаційний тероризм − це інформаційна складова усіх практичних протиправних дій терористів. Наприклад, якесь терористичне угруповання підриває пасажирський автобус і водночас те ж угрупування запускає в пресу інформацію, що буцім якщо уряд не піде на поступки терористів, вибухи триватимуть. Інформаційний тероризм завжди має публічний характер, і самі організатори терористичних актів прагнуть до максимального привертання уваги з боку засобів ЗМІ, а отже, − до суспільного резонансу [15; 27; 69; 72; 145].

Розрізняють міжнародний, внутрішньонаціональний регіональний і місцевий інформаційний тероризм.

Одним із найнебезпечніших проявів перелічених видів інформаційного тероризму є той, який переслідує екстремістські релігійні цілі. Наприклад, певне терористичне угрупування здійснює вбивство відомого релігійного діяча і починає поширювати інформацію про те, що це вбивство − справа рук

представників іншої релігійної громади. Засоби масової інформації починають тиражувати цю неправдиву інформацію і фактично беруть участь у провокуванні міжрелігійного або міжнаціонального конфлікту. При цьому можуть переслідуватися політичні або навіть кримінальні цілі [15; 27; 72; 145].

Здійснення інформаційного тероризму ведеться за допомогою політичних міркувань преси. Боротьба з інформаційним тероризмом повинна вестися безперервно, в першу чергу державними структурами, відповідальними за інформаційну безпеку країни. Метою інформаційної безпеки є забезпечення захисту життєво важливих інтересів особи, суспільства і держави від зовнішніх і внутрішніх загроз, до яких, зокрема, належать антидержавна й антигромадська діяльність окремих іноземних держав та внутрішніх суспільних і економічних структур в галузі продукування, розповсюдження і використання інформації.

Держава повинна визначити те, що підлягає інформаційному захисту від посягань. Головні місця серед об’єктів захисту посідають:

– конкретна інформація про діяльність того чи іншого актора;

– інформаційний простір країни в цілому;

– стратегічно важливі структури, а, саме, − система енергетичного забезпечення ядерних об’єктів, система управління повітряним транспортом та інші найбільш імовірні цілі для атак;

– державні бази даних і бази даних провідних економічних структур;

– найважливіші інформаційно-технічні системи [147; 149; 168; 309].

Політична система України принципово відрізняється від політичних систем розвинених країн тим, що досі остаточно не сформувалася, у нас і досі не завершився період переходу від радянської до демократичної системи державного правління. Зараз у нашій державі виконавча гілка влади домінує над законодавчою гілкою, яка замість контролю та інспектування діяльності виконавчих органів влади виступає в ролі глядача і проявляє пасивність.

Серйозною проблемою стала відсутність в Україні рівного доступу політичних партій до телебачення і взагалі можливості окремих політичних акторів вести свою інформаційну політику за допомогою державних засобів масової інформації. Будь-яку політичну партію насамперед цікавить можливість вести свою інформаційну політику всередині країни, а вже потім постає питання позиціонування себе на міжнародній арені.

Українські партії приділяють недостатньо уваги своїй інформаційній політиці, а що стосується роботи в регіонах, там пожвавлення починається тільки перед виборами і відразу ж після них закінчується. Механізм реалізації внутрішньої інформаційної політики українських партій вкрай не ефективний, оскільки не має систематичного характеру і не може задовольнити інформаційні потреби громадян у відомостях про діяльність основних політичних сил в країні. Про вищезазначене свідчить проведений нижче аналіз. Зокрема, у роботі здійснено розрахунок показника «зважені рейтинги» для політичної реклами на телебаченні [132].

Так, WGRP (англ. − Weighted Gross Rating Points) − зважені або наведені рейтинги, які являють собою умовні одиниці при придбанні реклами на телебаченні. Вони передбачають кількість глядачів, які мали контакт з рекламним роликом, приведеним до 30-ти секундного еквіваленту.

Рейтинг − це кількість людей (у відсотках або абсолютних цифрах), які мали контакт з подією, наприклад, з рекламним роликом. Але це визначення передбачає, що рейтинг від тривалості ролика не залежить. Тобто, якщо 10 % аудиторії побачили поспіль два рекламних ролики – один 5 секунд, а другий 30, це означає, що обидва мають рейтинг 10 %.

Для розрахунку WGRP треба рейтинг кожного ролика помножити на коефіцієнт ціни для тривалості цього ролика. За одиницю зазвичай встановлюється тривалість 30 секунд.

Наприклад, якщо на телевізійному канал використовується пропорційна систему коефіцієнтів, то для презентованого вище ролика WGRP (5 сек.) = $10\% \times \frac{5}{30}$ = 1,67 %.

Так, нижче доцільно проаналізувати зважені рейтинги для політичної реклами протягом останніх років в Україні. Зокрема, протягом 2008–2012 років динаміка зміни цього показника виглядає так, як показано у табл. 3.1 та на рис. 3.1 [308].

Таблиця 3.1

Динаміка зміни зважених рейтингів для політичної реклами протягом 2008–2012 років

Рік	WGRP, %
2008	5 400
2009	41 271
2010	30 661
2011	58
2012	68 417

Джерело: складено на підставі [308]

Нагадаємо, що протягом 2008 р. відбувалася передвиборча кампанія мера м. Києва, а у 2009 р. розпочалася виборча кампанія у Президенти України, яка тривала до 2010 р. Зрозуміло, що вказані події суттєво вплинули не лише на загальний обсяг політичної реклами, а й на час, коли трансляція відповідних політичних рекламних роликів була найактивнішою. Наступного року (2011) політичних кампаній в Україні не відбувалося, тому обсяг політичної реклами є незначним, натомість у 2012 виборча кампанія у народні депутати України спричинила суттєве підвищення обсягів політичної реклами. При цьому найбільша частка такої реклами транслювалася на телеканалі «Інтер».

Рис. 3.1. Тенденції зміни зважених рейтингів для політичної реклами протягом 2008–2012 років

Джерело: складено на підставі [308]

Що стосується 2019 року, то загальний обсяг політичної реклами на телебаченні у цьому році оцінюється у 1,2-1,5 мільярди гривень за підсумками двох ключових політичних кампаній – виборів Президента та Верховної Ради.

Що стосується обсягів політичної реклами в пресі та на радіо у грошовому вираженні, то орієнтовно їх можна оцінити у 50 млн. грн. та 70 млн. грн. відповідно. Обсяг зовнішньої політичної реклами склав 462 млн. грн. (табл. 3.2) [308].

Виникає таке відчуття, що політичні партії взагалі не цікавить робота в регіонах, та проведення інформаційної політики не міститься в списку їх першочергових завдань, оскільки у більшості партій немає сайтів в регіонах, хоча очевидно, що один центральний сайт не може відображати весь спектр політичних подій в Україні.

Таблиця 3.2

Розподіл обсягів політичної реклами за носіями рекламної інформації протягом 2019 року

Рекламний носій	Обсяг політичної реклами, млн. грн.
Телебачення	1 200 – 1 500
Зовнішні конструкції	462
Радіо	70
Преса	50

Джерело: складено на підставі [308]

Місцева преса, як правило, орієнтується на місцеві проблеми. Для багатьох регіонів сьогодні першорядної важливості набуває інформація, отримана переважно через канали регіональних і місцевих інформаційних джерел. В організації роботи прес-служби сучасної української партії примітним є те, що інформація, що стосується регіонів, перш за все повинна не надходити з центру, в інтерпретації столичних журналістів, а висвітлюватися місцевими фахівцями. Може здатися, що українські партії постійно відчувають нестачу фінансування і просто не в змозі виділити достатню кількість ресурсів для реалізації на належному рівні загальнодержавної та регіональної інформаційної політики. Це не відповідає дійсності, оскільки всі великі політичні партії в Україні отримують фінансову допомогу від бізнесменів, зацікавлених у просуванні (лобіювання своїх інтересів у вищих ешелонах влади) [205].

Взаємодія між бізнесом та інститутами влади існує в будь-якій країні. Але в більшості держав, насамперед у країнах розвиненої демократії, вона опосередкована політичними партіями.

Політичні партії, незалежно від того, чи вони підтримують уряд чи є опозиційними, повинні пам’ятати про свою відповідальність перед суспільством і вибудовувати свою внутрішню інформаційну політику так, щоб консолідувати суспільство, а не сприяти його розшаруванню. Особливе значення консолідація суспільства набуває в складні для держави і

суспільства періоди часу, коли треба, щоб усі громадяни об'єдналися перед спільною загрозою.

Інформаційна політика суб'єкта, що реалізує її в умовах глобалізації, провадитися з урахуванням того, що, діючи в інтересах певного суб'єкта, вона не лише актуалізує інтереси, присутні в геополітичному просторі існування цього конкретного суб'єкта, а й зачіпає інтереси значної кількості суб'єктів глобального світу. Через тісний зв'язок з глобалізацією інформація стала одним з найважливіших напрямів технічного прогресу взагалі, серед іншого в сфері управління та інформаційного забезпечення створення матеріальних та інтелектуальних благ.

Висновки до третього розділу

1. Підкреслено, що відповідно до Європейської конвенції про кіберзлочинність (інформаційну безпеку) забезпечення розглядуваного різновиду безпеки передбачало недопущення чи усунення таких суспільно-небезпечних діянь проти конфіденційності даних, як протиправний доступ, перехоплення, порушення цілісності, втручання в роботу, виробництво, обіг та використання спеціальних засобів для вчинення комп'ютерних злочинів з використанням комп'ютерів, підроблення та інформаційне шахрайство.

2. Показано, що в умовах існування великої кількості стандартів інформаційного забезпечення держбезпеки необхідно встановлювати зв'язки між ними, що, у свою чергу, зумовлює необхідність розроблення та впровадження певного метастандарту інформаційного забезпечення держбезпеки.

3. Обґрунтовано, що сьогодні слід визнати відсутність єдиного правового поля стосовно регулювання інформаційного забезпечення державної безпеки. Зазначено, що в різних нормативних правових актах перелічується велика кількість таємниць, проте за розголошення не всіх з них передбачено відповідальність. Крім того, відмічено, що сучасне

законодавство, яке регулює питання забезпечення інформаційної безпеки України, не розглядає її у форматі захисту інформаційної свободи.

4. Органи державної влади спеціальної компетенції, що регулюють інформаційну безпеку, поділено на групи залежно від певного виду інформаційних відносин, які зазнають інформаційного впливу. У результаті виокремлено такі їх групи:

– органи, які прямо впливають на сферу інформаційних відносин у загальному контексті та провадять державну інформаційну політику (Державний комітет телебачення і радіомовлення України);

– органи, що розробляють і провадять державну мовну політику та державну політику із захисту суспільної моралі (Міністерство культури України);

– органи, що в той чи інший спосіб регулюють отримання і зберігання інформації (Державний комітет статистики України та Державний комітет архівів України);

– органи, що відповідають за аналіз і моніторинг певних типів інформації (Державна служба фінансового моніторингу України).

Підкреслено, що цей підхід заважає повноцінно здійснювати забезпечення інформаційної безпеки в державі, відповідно, необхідно чітко визначити частку й межі державної участі в забезпеченні інформаційної безпеки, серед іншого шляхом законодавчого встановлення заборон та обмежень в розглядуваній сфері.

5. Визначено ключові складові системи інформаційних загроз для суспільства. До них належать: посилення психоемоційної напруженості в суспільстві, її нагнітання аж до руйнування психіки, масове використання технік маніпулювання та дезінформації, здатне заподіяти шкоду інтересам громадян, підміна культурних цінностей, що сформувалися, усталеної морально-етичної системи стандартів або релігійних вірувань, монополізація інформаційної сфери суспільства.

6. Доведено, що державна інформаційна політика держави має дві складові – техніко-технологічну та гуманітарну. Зокрема, зазначено, що техніко-технологічна складова є пов'язаною з інформатизацією суспільства; розвитком інформаційно-комунікаційних технологій і їх практичним використанням та створенням конкурентоспроможної інформаційно-технологічної інфраструктури. До гуманітарної складової розглядуваної політики держави належать зміст і якість інформації, використовувані в ній поняття, вплив цієї політики на політичні, соціальні та інші процеси в суспільстві тощо. Через це гуманітарну складову державної інформаційної політики доречно визнати визначальною.

7. Виокремлено низку напрямів забезпечення державою своєї інформаційної політики. Обґрунтовано, що найважливішими з них є фінансово-економічний, організаційно-технічний і правовий.

Зокрема, фінансово-економічні методи передбачають: удосконалення системи фінансування робіт з розроблення програм забезпечення інформаційної безпеки та створення системи страхування інформаційних ризиків фізичних і юридичних осіб.

Організаційно-технічні, відповідно, передбачають:

– створення і використання засобів захисту від несанкціонованого доступу до оброблюваної інформації;

– розроблення програм, які перешкоджають руйнуванню та викривленню інформації;

– покращення якості професійної та спеціальної підготовки користувачів інформаційних систем;

– постійне спостереження за діями обслуговуючого персоналу в захищених інформаційних системах.

Правова або законодавча діяльність держави щодо забезпечення інформаційної безпеки передбачає такі заходи:

а) розроблення законів та інших нормативно-правових актів, де передбачається відповідальність фізичних і юридичних осіб за

несанкціонований доступ до інформації; розголошення інформації, що містить державну або комерційну таємницю; викривлення, протизаконне використання або протиправне копіювання інформації; використання в злочинних цілях службової інформації; навмисне розповсюдження недостовірної інформації;

б) створення нормативно-правових актів, що обмежують частку іноземної участі у володінні загальнодержавними ЗМІ;

в) установлення законодавчого розмежування повноважень у галузі інформаційної безпеки між органами влади;

г) розроблення нормативно-правових актів щодо регламентації взаємовідносини держави з контрагентами (як поза межами держави, так і всередині неї) в інформаційній сфері.

РОЗДІЛ 4
РОЗВИТОК ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ФУНКЦІОНУВАННЯ ЦИФРОВОГО СУСПІЛЬСТВА

4.1. Інвентаризація та категоріювання інформаційних ресурсів у державному та регіональному інформаційному просторі

Важливість інформаційної безпеки серед іншого зумовлюється тим, що саме від її стану прямо залежить ефективність функціонування систем управління й у цілому будь-яких соціально-економічних комплексів [16; 22; 118; 208; 230; 263; 276; 309]. Такою безпекою зазвичай вважається стан захищеності інформаційного середовища у певній державі чи конкретному суспільстві, завдяки чому це середовище формується і розвивається в інтересах громадян, їхніх різноманітних груп (організацій) і цієї держави. Інформаційна безпека має тісний зв’язок із:

– правами особи, суспільства та держави на пошук, одержання і поширення достовірної інформації у будь-який законний спосіб і захистом цих прав;

– недоторканістю приватного життя, особистої, сімейної та державної таємниці;

– збереженням і примноженням культурних і духовно-моральних цінностей, історичних традицій, звичаїв та інших норм співжиття.

Вирішити такі складні завдання неможливо без участі органів місцевого самоврядування в системі забезпечення інформаційної безпеки України.

Зазначені напрями захисту інформації слід реалізовувати у конкретних видах діяльності, які виконують різні органи державної влади та місцевого самоврядування, підприємства, установи й організації відповідно до їх компетенції [77; 183].

Взаємозв'язок напрямків діяльності із забезпечення цієї безпеки і складності проблем, що виникають, вимагає скоординованих дій у цій сфері. Така координація не може здійснюватися лише органами виконавчої влади держави. Доцільніше створити систему координації діяльності в галузі інформаційної безпеки, розподілену за рівнями державного управління та місцевого самоврядування, що відображатиме науково-технічні, соціально-економічні й інші проблеми у розглядуваній сфері та їх структуру [46; 49; 71; 84; 161].

У цьому разі до основних координаційних проблем на рівні місцевого самоврядування пропонується віднести такі:

1) завчасне передбачення (прогнозування) загроз інформаційній безпеці та прорахунок їх наслідків в певному регіоні; розроблення моделей таких загроз стосовно різних напрямів забезпечення цієї безпеки, якими зможуть користуватися будь-які бажаючі незалежно від їх відомчої приналежності;

2) формування організаційно-правового ґрунту для захисту інформаційного простору в Україні (зокрема, з урахуванням особливостей різних її регіонів);

3) розроблення та провадження єдиної політики стосовно систематизації, обліку і забезпечення доступу до державних і недержавних інформаційних ресурсів регіону; розвиток регіональних і локальних підсистем захисту інформації від технічних розвідок і від її витоку крізь технічні канали [272];

4) розроблення і вдосконалення загальнодоступних інформаційно-комп'ютерних технологій, на які спиратимуться системи регіонального інформаційного простору;

5) виявлення шкідливих інформаційно-психологічних впливів на громадян через органи державної влади та місцевого самоврядування, що здійснюються різними каналами, та зупинення (локалізація) їх поширення;

6) ужиття узгоджених заходів з охорони і забезпечення стабільного функціонування найважливіших об’єктів інформаційної інфраструктури регіону в умовах загрози тероризму;

7) підготовка для регіону фахівців у галузі інформаційної безпеки, забезпечення для них підвищення кваліфікації.

Загалом необхідність інвентаризації інформаційних ресурсів у державному та регіональному інформаційному просторі, включно із захистом інформації й її категоріюванням [24; 29; 162], обумовлюються таким:

– необхідністю оцінювати небезпечність загроз витоку або пошкодження інформації;

– необхідністю прив’язки відповідних заходів і засобів безпеки до інформації, яка перебуває під захистом.

Тому далі під інвентаризацією державних і регіональних інформаційних ресурсів будемо розуміти процедуру аналізу інформації, що зберігається й обробляється на державному чи регіональному об’єкті інформатизації, в інтересах:

– віднесення її до інформації, яка підлягає захисту;

– поділу інформації на поіменовані блоки із забезпеченням можливості знаходження будь-якого блоку за його іменем під час вирішення завдань щодо захисту інформації.

При цьому під категоріюванням інформації, яка підлягає захисту, розуміється віднесення поіменованого блоку інформації до відповідної категорії із заздалегідь визначеного списку категорій. Зауважимо, що питання інвентаризації державних та регіональних інформаційних ресурсів і категоріювання інформації досі ні в теоретичному, ні в практичному плані достатньою мірою не досліджувалися [24; 29; 116; 162].

Відповідно до цього визначення процес інвентаризації інформації охоплює:

– визначення видів таємниць, які можуть розкриватися завдяки перехопленню чи виявленню змісту інформації на державному чи регіональному об’єкті інформатизації;

– кластеризацію всієї інформації, тобто поділ інформації на блоки й надання кожного блоку власної назви;

– поділ інформації на призначену для користувача і системну;

– виділення блоків користувальницької інформації, що належить до того чи іншого виду таємниці, поділ інформації користувачів за видами таємниць;

– оцінювання можливості розголошення інформації, що становить той чи інший вид таємниці, на держаному чи регіональному об’єкті інформатизації у процесі розмов в приміщеннях або із застосуванням засобів зв’язку;

– виділення блоків системної і користувальницької інформації, цілісність або доступність якої необхідно захищати;

– визначення носіїв інформації, що захищається.

При цьому ключовим етапом інвентаризації інформації є її віднесення до даних, що захищаються [25; 187]. Наразі в адміністративних і кібернетичних системах це здійснюється тільки в межах вирішення завдання щодо забезпечення конфіденційності інформації експертним шляхом на підставі встановлення відповідності інформації переліку відомостей, які належать до одного з видів таємниць. Для забезпечення цілісності або доступності інформації інвентаризація практично не проводилася. Однак без неї неможливо сформувати повний перелік актуальних загроз інформаційній безпеці на державному та регіональному рівні.

Зміст процедури віднесення інформації до даних, що захищаються, полягає в оцінюванні шкоди (зокрема збитків) від порушення її конфіденційності, цілісності чи доступу до неї. Для оцінювання збитків від порушення конфіденційності інформації, що належить до державної таємниці, а також у низці випадків оцінювання найбільш важливої

інформації, що належить до інших видів таємниць, використовується бінарний підхід, що ґрунтується на концепції неприйнятності ігнорування можливості витоку або розголошення інформації. Сенс цього полягає в тому, що якщо в блоці інформації є відомості, які відповідно до встановленого переліку належать до таємниці, то цей блок інформації належить до даних, що захищаються. При цьому може аналізуватися або семантика інформації, або можуть виявлятися спеціальні мітки на текстовій, графічній, аудіо або іншій інформації, за якими вона належить до даних, що захищаються [25; 187].

При цьому доцільно ввести такі правила для визначення важливості інформації в інформаційно-комп'ютерних технологіях органів державної влади та місцевого самоврядування:

– у випадках, коли у файлі (текстовому, графічному, файлі бази даних тощо) присутня інформація, що захищається, то весь файл підлягає захисту, і файлу присвоюється відповідний рівень важливості;

– градація важливості інформації з позицій забезпечення її конфіденційності повністю визначається присвоєним їй грифом секретності або конфіденційності. Зокрема, для конфіденційної інформації гриф конфіденційності визначається залежно від того, яке коло осіб має право ознайомлення з нею, і визначається переважно користувачем такої інформації;

– градація важливості інформації з точки зору забезпечення її цілісності або доступності визначається користувачем і залежить від рівня і прийнятності витрат (часу, трудових ресурсів, фінансових ресурсів тощо) на відновлення цілісності або доступності інформації;

– виконувані файли прикладних програм, запуск яких обумовлює доступ до файлів з даними користувача, мають велику важливість (з точки зору забезпечення як їх цілісності, так і доступності), ніж самі файли з даними користувача;

– файли інформації, порушення цілісності або доступності яких призводить до зриву роботи операційної системи регіональної інформаційно-комп'ютерної системи, мають велику важливість з точки зору забезпечення їх цілісності або доступності, ніж інші файли, що зберігаються в системі;

– якщо в приміщенні адміністрації органів державної влади чи місцевого самоврядування зберігається конфіденційна інформація, або приміщення виділено для конфіденційних переговорів, то вважається, що інформація, розповсюджена у процесі розмов посадовців або під час передання по лініях зв'язку, має вищий рівень конфіденційності, передбачений для цього приміщення, тобто відбувається можливий витік інформації з найбільшим рівнем важливості для адміністрації [25; 187].

При цьому для градації важливості інформації виділяються такі рівні.

I. В інтересах забезпечення конфіденційності інформації:

1) перший рівень − для інформації, що містить відомості особливої важливості;

2) другий рівень − для тієї, що містить цілком таємні відомості:

3) третій рівень − для інформації, що містить секретні відомості;

4) четвертий рівень − для конфіденційної інформації із відомостями, що належать до службової, комерційної або інших видів таємниць, віднесеної користувачем до особливо конфіденційної (з нею мають право ознайомитись тільки вищі посадові особи органів державної влади чи адміністрації місцевого самоврядування);

5) п'ятий рівень − для конфіденційної інформації, віднесеної до абсолютно конфіденційної (з нею мають право ознайомитися особи керівного складу адміністрації місцевого самоврядування);

6) шостий рівень − для конфіденційної інформації, віднесеної до звичайної конфіденційної інформації підприємства, установи чи організації (з нею мають право ознайомитися особи, склад яких визначається головою адміністрації місцевого самоврядування);

7) сьомий рівень − для конфіденційної інформації, віднесеної самим користувачем до конфіденційної (з нею мають право ознайомитися особи, склад яких визначено самим користувачем) (рис. 4.1).

II. В інтересах забезпечення цілісності інформації:

1) перший рівень − для інформації, порушення цілісності якої є недопустимим;

2) другий рівень − для тієї, порушення цілісності якої спричинює значні витрати для органів державної влади чи адміністрації місцевого самоврядування або користувача, проте саму таку інформацію частково або повною мірою можна відновити;

3) третій рівень − для такої, порушення цілісності якої є небажаним, однак у разі її порушення інформацію можна відновити з незначними витратами (рис. 4.2);

III. В інтересах забезпечення доступності інформації:

1) перший рівень − для інформації, порушення доступності якої є неприйнятним;

2) другий рівень − для такої, порушення доступності якої призводить до значних втрат, проте доступність якої можна частково або повною мірою відновити;

3) третій рівень − для такої, порушення доступності якої є небажаним, однак у разі її порушення інформацію можна відновити без значних витрат (рис. 4.3).

Запропонований підхід є оригінальним і дозволяє на формальному рівні вирішувати питання інвентаризації та категоріювання інформації в інтересах забезпечення державної системи інформаційної безпеки, насамперед для захисту регіонального інформаційно-кібернетичного простору [25; 187].

Формування переліків відомостей, віднесених до інформації обмеженого доступу, має ґрунтуватися на принципах законності, обґрунтованості і своєчасності вжиття заходів для захисту відомостей.

Зокрема, принцип законності полягає в урахуванні під час формування зазначених переліків відомостей вимог як правових документів, що обмежують доступ до інформації, так і документів, що забороняють вводити такі обмеження.

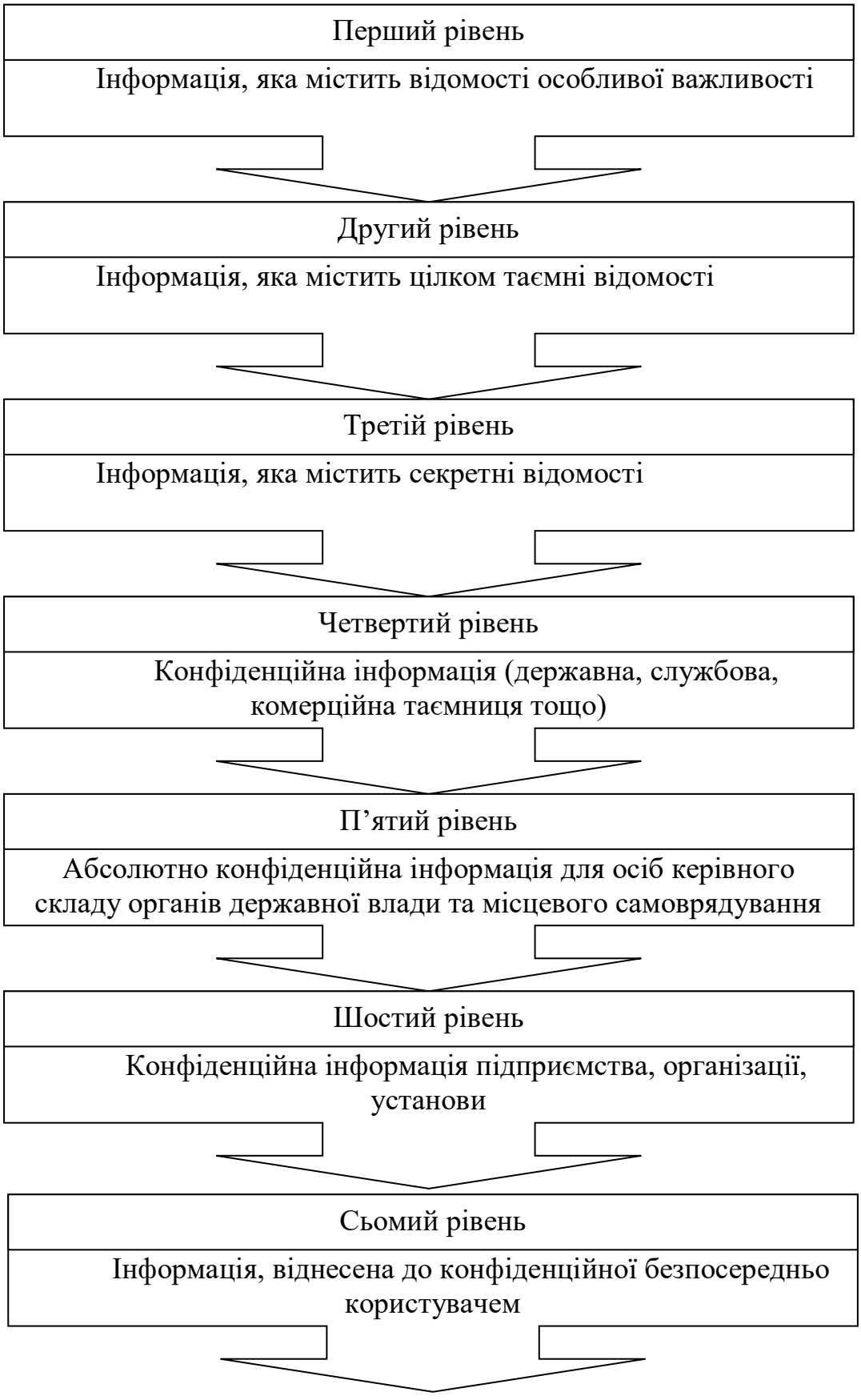

Рис. 4.1. Рівні градації забезпечення конфіденційності інформації, що підлягає захисту

Джерело: авторська розробка

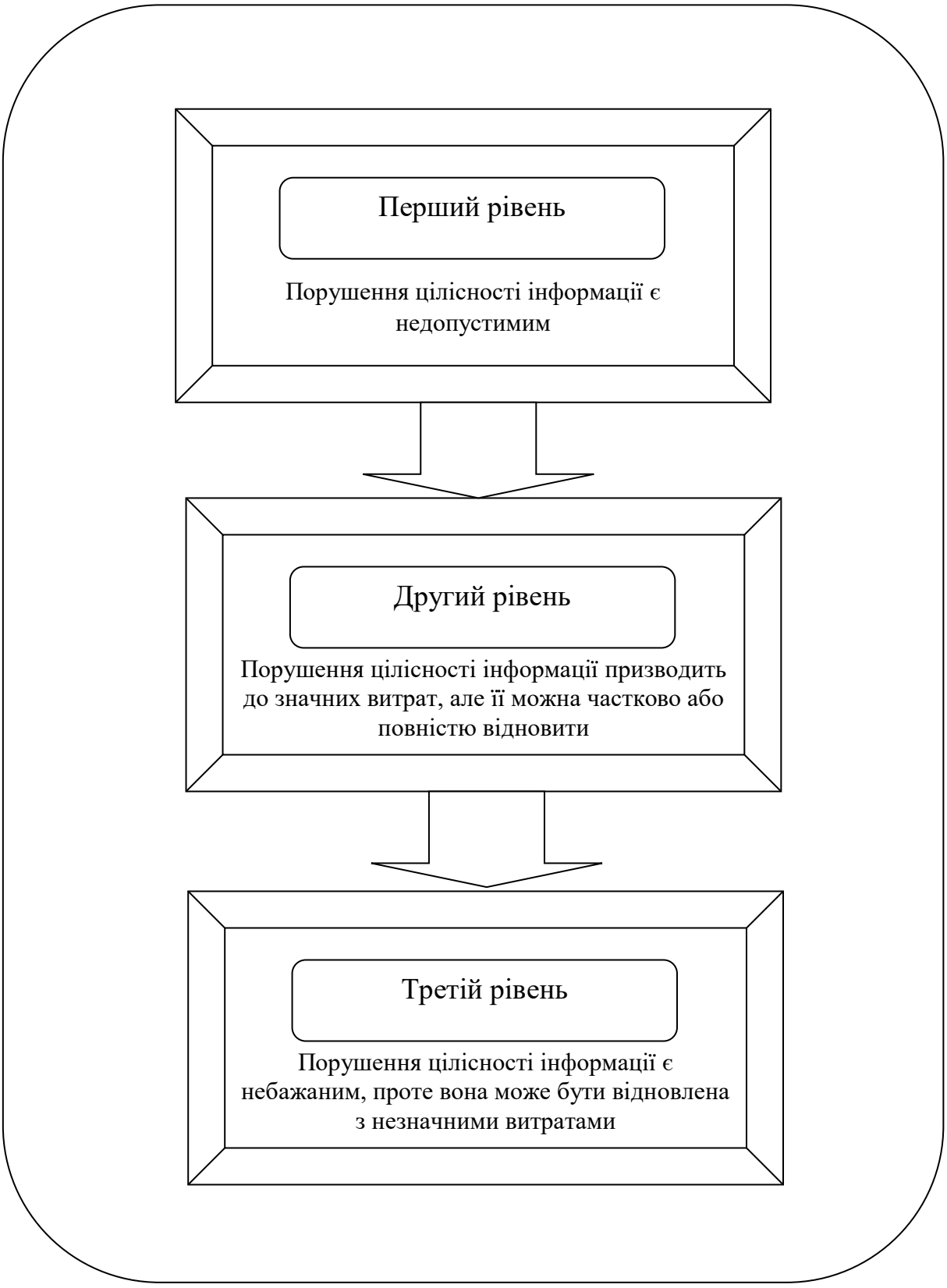

Рис. 4.2. Рівні градації забезпечення цілісності інформації, що підлягає захисту

Джерело: авторська розробка

Рис. 4.3. Рівні градації забезпечення доступності інформації, що підлягає захисту

Джерело: авторська розробка

Принцип обґрунтованості полягає в ухваленні рішення про обмеження розповсюдження відомостей з урахуванням всебічного оцінювання усіх боків цього акту – як позитивних, так і негативних. При цьому запровадження обмежень на поширення відомостей на певний термін часу покликане сприяти ефективнішому використанню інформації.

Принцип своєчасності полягає у встановленні обмежень щодо розповсюдження інформації обмеженого доступу з моменту її отримання (розроблення) або завчасно. Водночас цей самий принцип означає необхідність завчасно розробляти заходи щодо захисту інформації та можливості їх оперативного коригування в разі зміни загроз, умов захисту і важливості інформації, що захищається. Реалізація цього принципу вимагає створення гнучкої керованої системи захисту інформації, відповідальної за прогнозування і виявлення загроз, їх попереджувальну нейтралізацію та швидку ліквідацію наслідків їх реалізації. Виконати ці завдання суттєво допомагає запровадження системи моніторингу стану систем інформаційної безпеки регіонального рівня.

Указані вище принципи реалізує описаний нижче алгоритм обґрунтування переліків відомостей, віднесених до інформації обмеженого доступу.

На першому етапі цього алгоритму здійснюється аналіз документованої інформації, що циркулює в установі, і проводиться її опис.

Як характеристики опису при цьому використовуються такі:

– найменування департаменту, комітету, підрозділу, що володіє інформацією;

– вид власника інформації: держава, муніципальне утворення, юридична чи фізична особа;

– зміст інформації (постанови, розпорядження чи інші рішення органів державної влади й органів місцевого самоврядування, документи нарад, проведених в установі чи департаменті, підсумки роботи цієї установи чи цього департаменту, прогнози соціально-економічного розвитку, плани роботи установи тощо) [25; 187].

На другому етапі формується клас інформаційних ресурсів, у яких зберігаються відомості, що належать до державної таємниці й мають бути засекречені відповідно до Закону України «Про захист державної таємниці».

Водночас формується клас інформаційних ресурсів, обмежувати доступ до яких заборонено на законних підставах (відомості про стан економіки чи злочинності; відомості, які не можуть вважатися комерційною таємницею тощо).

На третьому етапі визначаються класи інформаційних ресурсів, що містять відомості, які є таємницю юридичних і фізичних осіб (комерційну, банківську, особисту й інші види таємниць), передані цими особами в установу. Такі відомості необхідно обов’язково включати до переліку відомостей, віднесених до інформації обмеженого доступу, якщо їх конфіденційність встановлено власниками на законній підставі.

На четвертому етапі класи інформаційних ресурсів, розроблених в установі, що залишилися, аналізуються для виявлення можливих позитивних і негативних наслідків від запровадження обмежень на їх поширення. Для цього оцінюється величина шкоди, яку необхідно попередити, у разі введення обмежень на поширення відповідних відомостей, та витрати у вигляді упущеної вигоди вільного використання інформації, що при цьому виникають, а також витрати на її захист [25; 187]. Схему зазначеного вище алгоритму обґрунтування переліків відомостей, віднесених до інформації обмеженого доступу (поширення), показано на рис. 4.4.

Обмежувати поширення зазначених відомостей доцільно, якщо існують певні схеми їх розповсюдження і термін обмеження вільного доступу, за яких величина шкоди, що попереджається, перевищує величину витрат, рівних сумі упущеної вигоди (можливостей) від їх відкритого використання і витрат на захист.

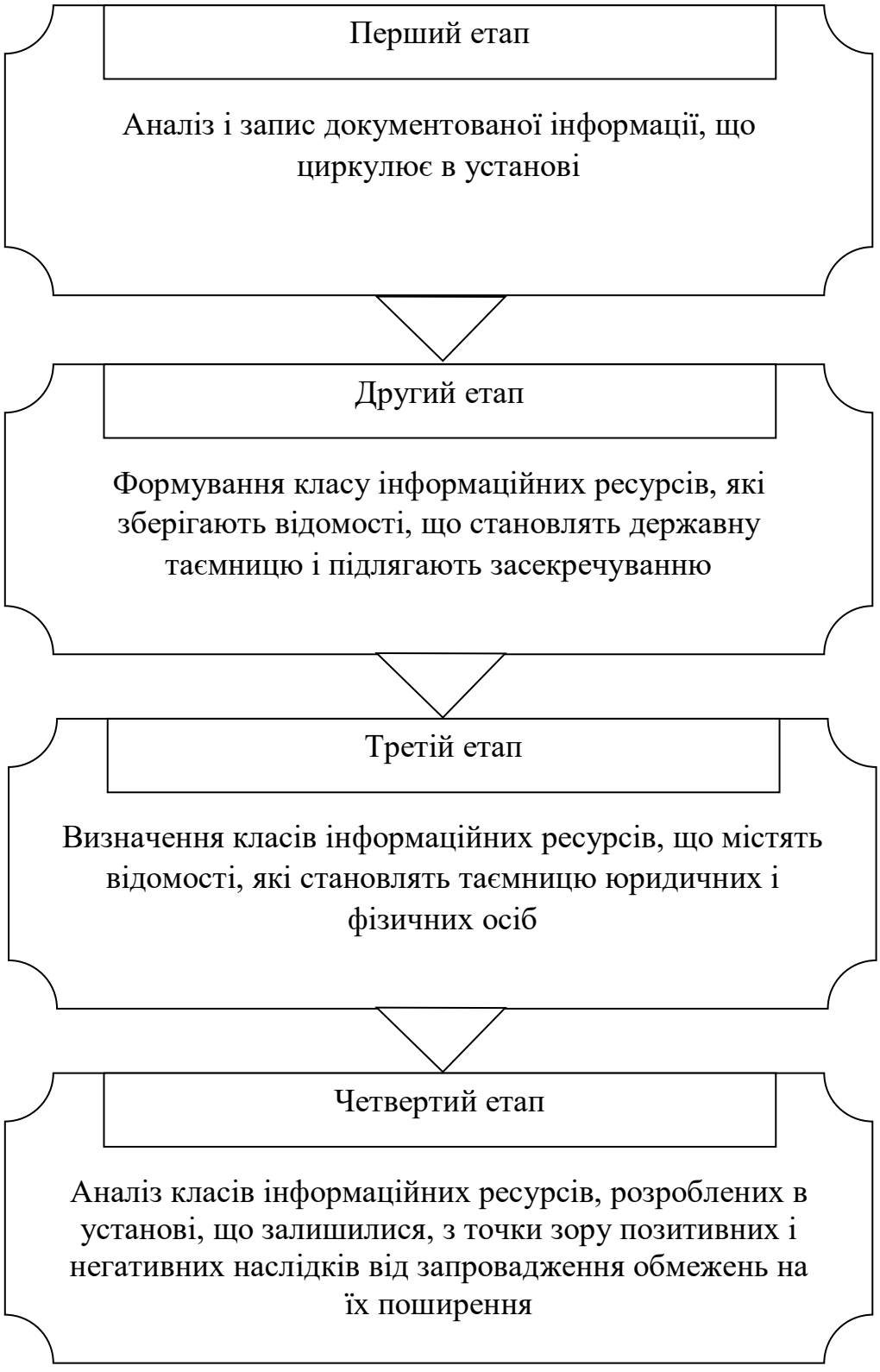

Рис. 4.4. Алгоритм обґрунтування переліків відомостей, віднесених до інформації обмеженого доступу

Джерело: авторська розробка

У результаті класифікації можна виділити такі класи інформаційних ресурсів, що циркулюють в установі:

1) ресурс, що містить відомості, які становлять державну таємницю;

2) ресурс, що містить відомості, які становлять таємницю юридичних осіб (банківську, комерційну й іншу), що передали цю інформацію в установу;

3) ресурс, що містить відомості, отримані (розроблені) в установі, які становлять його службову, професійну або іншу таємницю;

4) ресурс, що містить відомості, що становлять таємницю фізичних осіб, серед іншого персональні дані;

5) ресурс, що містить відомості, поширення яких може заподіяти шкоду безпеці України, але які неможливо ідентифікувати з відомостями, згаданими в чинних списках відомостей, що належать до державної таємниці;

6) ресурс є відкритим, але цінним і тому вимагає захисту від знищення, перекручення, підробки чи блокування;

7) ресурс є відкритим і малоцінним та потребує додаткових заходів захисту.

Перелічені вище п’ять класів містять інформацію обмеженого доступу, що зумовлює необхідність її захисту від витоку, серед іншого через технічні канали. Відповідно до цієї класифікації складаються переліки інформаційних ресурсів обмеженого доступу, переліки відомостей обмеженого доступу, що їм відповідають (ті, які підлягають засекречуванню, становлять службову таємницю або інші види таємниць) і переліки загальнодоступних

інформаційних ресурсів, які необхідно захищати від несанкціонованих і ненавмисних дій через важливість цих ресурсів [25; 187].

Для класифікації інформації повинні створюватися експертні комісії з фахівців основних підрозділів установи, а також підрозділів захисту державної таємниці та інформації.

У цілому кількісно оцінити всі позитивні й негативні наслідки від обмеження поширення інформації досить складно. Треба усвідомлювати, що ці наслідки можуть спостерігатися в будь-яких сферах діяльності установи та оцінюватися в різних шкалах та в різних одиницях вимірювання. Для визначення інтегрального ефекту від запровадження обмежень на поширення інформації необхідно звести окремі оцінки до єдиної шкали, якою може служити відносна важливість наслідків, що розраховується методом експертних оцінок на основі парних порівнянь.

Вибір методу експертних оцінок обумовлюється відсутністю, в більшості випадків, елементарних вимірних властивостей можливих збитків і вигод, а також статистичних даних про їх прояв. Для зіставлення різних відомостей у межах з'ясування необхідності обмеження доступу до них пропонується оцінювати ці відомості за ступенем прояву всієї сукупності загроз у разі їх поширення і можливих витрат (упущеної вигоди і витрат) у разі обмеження доступу до них. У цьому випадку виникає завдання ранжування або визначення «ваги» загроз, вигод і витрат із тим, щоб отримати єдину міру, що характеризуватиме інтегральний ефект від обмеження поширення відомостей.

Для виконання цього завдання необхідно заздалегідь скласти переліки можливих загроз від несанкціонованого поширення інформації, вигод (переваг) вільного поширення інформації та статей витрат на її захист. Під час оцінювання інтегрального ефекту від обраного рішення поширення інформації необхідно зважати не лише на співвідношення між розміром («вагою») збитків, вигод і витрат, але і на тимчасові характеристики їх виникнення.

Наприклад, вигода відкритого використання інформації може проявитися досить швидко порівняно з часом виникнення шкоди власнику від дій недружніх суб'єктів, але збитки від відкриття інформації можуть значно перевершувати вигоду, що досягається. Обмеження ж поширення інформації на якийсь час може дозволити за незначного зниження розміру вигоди істотно знизити зазначену шкоду за рахунок того, що дії, які реалізуються недружнім суб'єктом, будуть невчасними і тому неефективними. Урахувавши усі ці чинники, необхідно вибрати такий режим поширення інформації, який на кінець періоду її активного життєвого циклу забезпечував би максимальний ефект від її використання.

Для визначення «ваги» збитків, вигод і витрат здійснюється їх парне порівняння відомим методом Т. Сааті за допомогою експертів, які добре розуміють цінність відомостей і їх взаємозв'язок із зазначеними чинниками [17]. Можливість їх прояви в динаміці життєвого циклу інформації оцінюється суб'єктивною ймовірністю.

Якщо розраховане значення інтегрального показника виявляється більшим за нуль, то включати розглянуту інформацію до переліку відомостей, доступ до яких обмежено, доцільно.

Відносити інформацію до інформаційних ресурсів, які слід захищати від несанкціонованих і ненавмисних дій, є сенс тоді, коли при цьому розмір шкоди, яку слід відвернути, перевищує величину витрат на її захист.

У відповідності до схеми збирання інформації оцінювання стану регіональної системи інформаційної безпеки слід здійснювати послідовно, починаючи з нижнього рівня ієрархії за окремими підсистемами, з узагальненням результатів оцінювання на вищому рівні. Зокрема, таке оцінювання має містити в собі оцінювання стану інформаційної безпеки на об'єктах захисту.

В узагальненому вигляді вимоги до забезпечення інформаційної безпеки на конкретному об'єкті охоплюють вимоги щодо організації процесу її забезпечення, включно з вимогами до матеріально-технічного, нормативно-

методичного, інформаційного, фінансового тощо забезпечення на об’єкті процесу підтримання такої безпеки.

Конкретний зміст вимог визначається на підставі чинних документів з урахуванням змісту відомостей про конкретний об’єкт, що підлягають охороні, та можливостей їх отримання конкуруючою стороною [274].

Для спрощення розрахунків можна вважати, що вимоги забезпечення інформаційної безпеки на об’єкті захисту не виконуються, якщо не виконується хоча б одна із зазначених окремих вимог. Однак такий підхід до оцінювання стану захисту є надмірно жорстким. Аналіз практики організації забезпечення інформаційної безпеки на різних об’єктах доводить, що якісь порушення в організації та здійсненні процесу захисту трапляються на більшості об’єктів. До того ж самі порушення за ступенем небезпечності, з точки зору витоку інформації, що захищається, можуть належати до різних категорій важливості. Так, порушення заходів забезпечення інформаційної безпеки, що становить державну таємницю, за ступенем небезпечності поділяються на три категорії:

1) перша − невиконання вимог або норм забезпечення інформаційної безпеки, через що виникала або існує реальна можливість її витоку технічними каналами, несанкціонованого доступу до неї або впливу на неї;

2) друга − невиконання вимог до забезпечення такої безпеки, внаслідок чого створюються передумови до її витоку технічними каналами або несанкціонованого доступу до неї;

3) третя – інші випадки невиконання вимог до забезпечення інформаційної безпеки.

4.2. Модернізація єдиної державної політики у сфері інформаційної безпеки

Через те, як змінилася роль інформації для всього людства, та через появу нових технологій обробки, передання, зберігання та подання

інформації стало можна стверджувати, що сучасна цивілізація не лише змінює свій вигляд, − вона входить в нову епоху, перетворюючись на інформаційну цивілізацію.

У нинішніх умовах колишній адміністративний механізм управління інформаційною безпекою став неефективним і не може повноцінно діяти. У безпосередньому підпорядкуванні органів державної влади та місцевого самоврядування України перебувають одиниці відсотків підприємств, установ та організацій, розташованих на їх території. За цих умов необхідність міжвідомчої координації щодо інформаційної безпеки об'єктивно зросла. Відповідно, актуальними є формування та реалізація єдиної державної політики у розглядуваній сфері [11; 12].

Наразі уже немає сумнівів, що технології інформаційного століття різною мірою охопили індустріальні, постіндустріальні й індустріальні країни.

Не випадково частина науковців в історії людського суспільства виділяє лише три основні стадії (за іншим формулюванням «хвилі»):

1) аграрна стадія (хвиля) – до XVIII століття);

2) індустріальна стадія (хвиля) – до 50-х років XX століття;

3) постіндустріальна стадія (хвиля) – починаючи з 50-х років XX століття [82; 342].

Це дозволяє окреслити головні риси постіндустріального суспільства, відштовхуючись від особливостей найбільш вивченої індустріальної стадії. У цьому контексті індустріальне суспільство трактується як суспільство, головною метою якого є виробництво якомога більшої кількості речей і механізмів. Відмінною рисою постіндустріальної стадії є зміщення цілі від їх виробництва на розвиток сфери послуг, пов'язаних з освітою, охороною здоров'я, науковими дослідженнями й управлінням [342].

Величезне значення в розвитку цих змін виникнення нового типу цивілізації − цивілізації третьої хвилі – має інформація [82].

З приходом цивілізації третьої хвилі інформаційну революцію багато хто вже визнав новим етапом науково-технічної революції, в результаті якої принципово змінюється роль інформаційної індустрії. Завдяки вдосконаленню новітніх інформаційних і телекомунікаційних технологій сформувалися безпрецедентні можливості щодо створення інформаційних продуктів − продуктів іншого типу, ніж в індустріальній цивілізації [119].

Таким чином, революційний характер і досягнення в інформаційній сфері стають передумовами руху до появи у XXI столітті принципово нового типу суспільства – інформаційного (за іншим формулюванням «суспільства знання»). Особливою, специфічною і характерною цього суспільства є його глобальний характер. Сьогодні у процесі його становлення поступово зменшуються кордони між людьми і різними державами, але найсильніші зміни відбуваються у структурі всесвітньої економіки. Такі принципові зміни, породжені прогресом інформаційних і телекомунікаційних технологій, стали предметом особливої уваги вчених, політиків і фахівців, особливо тих, чиї інтереси прямо стосуються питань, пов'язаних з інформацією. Саме з урахуванням формування цього суспільства в Україні і доречно досліджувати проблему інформаційної безпеки [2; 26; 78; 80; 231; 254; 256; 319].

Інформаційним суспільством заведено вважати такий його якісний стан, за якого суспільство, спираючись на згадані технології, досягає високого рівня політичного, економічного, науково-технічного і культурного розвитку. У цьому суспільстві бурхливо зростає обсяг інформації, що впливає на всі прояви його матеріального і духовного життя. ЗМІ стають тут надзвичайно важливими в контексті впливу на політичні процеси [2; 26; 51; 78; 123; 212; 231; 255; 256; 305; 318; 319].

Згаданий стрімкий розвиток інформаційно-телекомунікаційних технологій і їх конвергенція, що потягли за собою революційні зміни на світовому ринку, потребують удосконалення засобів роботи з інформацією (починаючи з її одержання й закінчуючи поширенням) та результатів їх використання, зокрема в економічній сфері. Практично саме радикальні

зміни самих інформаційних технологій наприкінці XX століття спричинили нову соціальну революцію глобальних масштабів, що не могло не відбитися на поширенні ідей глобального інформаційного суспільства [26; 319].

Паралельно з розвитком електронних ЗМІ й інформаційних технологій в науці дедалі активнішою стає дискусія щодо значення, ролі, завдань та функцій інформації в сучасній цивілізації, а також про тенденції становлення глобального інформаційного суспільства. При цьому головним чинником, що є ключовим для формування соціально-економічного підґрунтя цього суспільства, визнаються інформаційні технології. Можна провести аналогію між телекомунікаційними й комп'ютерними мережами та нервовою системою, адже саме завдяки ним всі складові світу стають тісно пов'язаними, завдяки чому і розвивається глобальна інформаційна система [31; 43; 78; 318].

Стосовно перспектив розвитку засобів масової комунікації в такому суспільстві особливої уваги заслуговує тенденція підвищення вагомості ролі мас-медіа, адже вони не лише виокремились в особливу сфера суспільного життя, а й поступово перетворюються на силу, влада якої над суспільством неухильно збільшується [117].

У контексті виділення в історії розвитку цивілізації згаданих вище трьох хвиль, також вважається, що постіндустріальному суспільству притаманні такі риси:

– деконцентрація населення і виробництва;

– різке посилення обміну інформацією;

– переважання самоврядних політичних систем;

– посилення індивідуалізації особи зі збереженням солідарних відносин між людьми і спільнотами.

Традиційним корпораціям протиставляються малі економічні форми, серед яких особливо виділяється індивідуальна діяльність на дому і «електронний котедж».

Підсумовуючи розглянуті тлумачення терміна «глобальне інформаційне суспільство», можна зробити висновок, що наразі під ним мається на увазі новий тип суспільства, що почав складатись і розвиватись унаслідок нової глобальної цивілізаційної революції, головною причиною якої стали стрімкий розвиток інформаційних і комунікативних технологій і їх конвергенція [2; 78; 212; 318].

Узагальнюючи викладене вище, підкреслимо, що з настанням нової епохи розвитку людської цивілізації (що зводиться до переходу до інформаційного суспільства), поступово змінюються всі без винятку сфери життя людини і суспільства. Важливими складовими змісту прийдешньої епохи є насамперед нові інформаційні технології, що радикально змінюють внутрішню структуру людської цивілізації, її зміст і навіть зовнішній вигляд. Саме тому вкрай важливим завданням нині є вивчення сутності та змісту нашої вітчизняної внутрішньої і зовнішньої політики в контексті цих глобальних змін усієї людської цивілізації [319].

При цьому аналіз поточних проблем інформаційної безпеки в Україні прямо вказує на необхідність її забезпечення й вимагає невідкладного вирішення низки таких завдань:

– формування провідних напрямків політики держави стосовно забезпечення інформаційної безпеки; розроблення заходів і створення механізмів, необхідних для реалізації цієї політики;

– подальше удосконалення вітчизняної системи забезпечення такої, в якій втілюватиметься відповідно єдина державна політику, включно з удосконаленням форм, методів і засобів виявлення, оцінювання та прогнозування загроз інформаційній безпеці України й розбудовою системи протидії цим загрозам;

– започаткування державою цільових програм із забезпечення такої безпеки;

– розроблення критеріїв і методів оцінювання ефективності систем і засобів її забезпечення, а також необхідного наукового й законодавчого забезпечення сертифікації цих систем і засобів;

– оновлення законодавчої і нормативно-правової бази забезпечення інформаційної безпеки, включно з механізмами реалізації прав громадян на отримання інформації та доступ до неї та формами і способами реалізації правових норм, що стосуються взаємодії держави із ЗМІ;

– налагодження у сфері забезпечення інформаційної безпеки координації діяльності між українськими органами державної влади та місцевого самоврядування, підприємствами, установами та організаціями незалежно від форми власності;

– подальше вдосконалення науково-практичного підґрунтя забезпечення такої безпеки, що враховуватиме сучасну геополітичну ситуацію, особливості політичного і соціально-економічного розвитку України та небезпеки застосування проти неї інформаційної зброї;

– поступове практичне формування механізмів розроблення та реалізації державної політики в інформаційній сфері;

– пошук та/або розроблення методів посилення ефективності участі держави у формуванні інформаційної політики державних телерадіомовних організацій та інших державних ЗМІ;

– досягнення технологічної незалежності України в найважливіших сферах інформатизації, телекомунікації і зв’язку, від яких залежить її безпека, насамперед у галузі створення спеціалізованої обчислювальної техніки для озброєння і військової техніки;

– удосконалення методів і засобів захисту інформації, забезпечення безпеки інформаційних технологій, які застосовуються в військовій галузі (зокрема в системах управління військами і зброєю), а також на екологічно небезпечних та ключових для економіки виробництвах;

– подальше вдосконалення і розширення державних систем захисту інформації взагалі та державної таємниці зокрема;

– сприяння активному розвитку вітчизняної інформаційної інфраструктури, участі нашої держави у розбудові та використанні глобальних інформаційних мереж і систем;

– запровадження єдиної системи підготовки кадрів у сфері інформаційної безпеки й інформаційних технологій [43; 78; 159].

Також підкреслимо, що відсутність на законодавчому рівні достатніх гарантій захисту людини від загроз, пов'язаних з негативними інформаційними впливами, вимагає активно розробляти національне законодавство та норми міжнародного права, пов'язані із захистом психіки людини від негативних інформаційно-психологічних впливів. Через це маємо визнати, що стан справ у цій галузі вимагає термінового вжиття практичних заходів для послаблення згаданих впливів. Тож, одним із найактуальніших завдань для вчених, політиків і державних діячів стає формування в національних інтересах держави ефективної комплексної (як внутрішньої, так і зовнішньої) державної інформаційної політики, що стане інструментом регулювання взаємодій між різними складовими суспільно-політичної системи. Це сприятиме і виконанню найважливішого із актуальних завдань, яким лишається збереження територіальної цілісності і суверенітету України [159].

Варто при цьому враховувати, що в сучасних умовах саме інформаційні війни, які містять у собі інформаційно-психологічну і технічну складові, становлять одну з головних загроз національній безпеці нашої держави. Разом із тим посилюється необхідність нарешті виробити в Україні принципово нову інформаційну політику, яка захищатиме інтереси держави і створюватиме умови, сприятливі для функціонування всієї системи інформаційної безпеки, але насамперед забезпечуватиме захист політичних, економічних та інших інтересів держави в розглядуваній сфері [5; 56; 98; 109; 150; 159].

Відповідно, у процесі формування та реалізації такої державної політики в інформаційній сфері необхідно:

– здійснювати збір, систематизацію й узагальнення інформації про стан інформаційної безпеки на об’єктах управління, оцінювання її стану в регіонах, виявлення невирішених проблем щодо її забезпечення, надання необхідної інформації про неї органам державної влади та місцевого самоврядування;

– контролювати стан такої безпеки на об’єктах управління;

– визначити пріоритетні напрямки забезпечення інформаційної безпеки як для держави в цілому, так і для конкретних регіонів;

– розробляти цільові програми із забезпечення інформаційної безпеки та контролювати їх виконання;

– здійснювати організацію науково-технічних досліджень і розробок в інтересах забезпечення такої безпеки в державі та регіонах, виконувати вимоги нормативних документів щодо її забезпечення;

– розробляти та затверджувати регіональні нормативні та методичні документи, присвячені забезпеченню цієї безпеки (концепції, положення, вимоги, норми, моделі, методики, рекомендації, інструкції та інші документи);

– надавати підприємствам, установам та організаціям методичну допомогу в підготовці до ліцензування, а також у діяльності, що стосується надання послуг у розглядуваній сфері, створення засобів інформаційної безпеки, впровадження засобів контролю їх ефективності тощо;

– здійснювати методичне керівництво професійною підготовкою фахівців у розглядуваній сфері, їх перепідготовкою та підвищенням кваліфікації;

– координувати дії органів місцевого самоврядування щодо створення муніципальних систем інформаційної безпеки [56; 150; 159].

Отже, можна виокремити такі принципові особливості процесу формування та реалізації єдиної державної політики у розглядуваній сфері:

– вона формується в межах державної системи забезпечення інформаційної безпеки;

– головними методами управління у зазначеному контексті виступають координація та регулювання діяльності із забезпечення такої безпеки;

– головним завданням розроблення та реалізації єдиної державної політики у цій сфері є створення і вдосконалення відповідних механізмів забезпечення інформаційної безпеки у межах компетенції різних органів державної влади та місцевого самоврядування [8; 12; 35; 90; 92; 266; 273].

Зауважимо, що органи державної влади й управління, уповноважені регулювати соціально-політичні відносини в інформаційно-психологічній сфері, разом із недержавними суб'єктами цієї діяльності, яких згадані вище органи залучають до вирішення завдань державного регулювання в указаній сфері, вважаються *суб'єктами державної інформаційної політики*. Водночас *суб'єктами забезпечення інформаційної безпеки* визнаються лише органи, організації та особи, уповноважені законом на здійснення відповідної діяльності [8; 22; 49; 67; 103; 124; 141; 146; 159; 208; 239].

Серед них можна виділити такі три основні типи (розрізняються за інтересами в здійсненні цієї діяльності):

1) індивіди як особистості;

2) громадські організації;

3) органи державної влади [22; 67; 103; 159; 208].

У свою чергу, всі суб'єкти державної інформаційної політики належать до однієї з двох основних категорій:

1) державні суб'єкти такої політики;

2) суб'єкти масового інформування і комунікації.

Також у системі суб'єктів цієї політики можна виокремити категорії державних суб'єктів за такими ознаками:

– рівні влади й управління (державний, регіональний, місцевий);

– гілки державної влади (законодавча, виконавча, судова);

– напрямки діяльності (органи цивільного чи економічного управління, «силовий блок», зовнішньополітичні відомства, відповідальні за культуру тощо) [67; 159; 329].

У свою чергу, суб'єкти масового інформування та комунікації в системі згаданих вище суб'єктів відповідної державної політики групуються за такими ознаками:

– за видом власності (державні ЗМІ, що контролюються українськими фізичними й юридичними особами; недержавні ЗМІ, що контролюються іноземними фізичними й юридичними особами; недержавні ЗМІ);

– за способом поширення інформації (електронні, друковані, інтернет-ЗМІ) [8; 159; 329].

При цьому держава посідає особливе місце серед обох основних категорій суб'єктів (і державної інформаційної політики, і забезпечення інформаційної безпеки), завдяки тому, що має унікальні засоби, сили і можливості протидії загрозам у цій сфері. Свою діяльність держава здійснює спільно з індивідами і суспільством, але при цьому її вплив на забезпечення інформаційної безпеки є визначальним. Із цього виливає, що всі проблеми захисту життєво важливих інтересів України в розглядуваній сфері мають вирішувати саме органи державної влади, хоча окремі свої функції у цій галузі держава реалізовує через органи законодавчої, виконавчої та судової влади.

Головною відмінністю держави від решти суб'єктів у розглядуваній сфері є те, що вона має монополію на насильство як засіб політичного домінування, великий набір засобів впливу на поведінку всіх членів суспільства, який можна творчо застосовувати, а також матеріальні, технічні та кадрові ресурси для реалізації своєї політики [368].

Усі органи держави так чи інакше беруть участь у забезпеченні інформаційної безпеки, однак їхні компетенція і предмети відання в цій сфері суттєво відрізняються, що визначається цілями, завданнями і компетенцією цих органів [8; 159; 333].

Саме компетенція цих органів є тим фундаментом, на якому будується вся система забезпечення розглядуваного різновиду безпеки. Оскільки інформаційні системи й інформаційні ресурси створюються і використовуються всіма органами державної влади, в системі забезпечення інформаційної безпеки особливу роль відіграють ті з них, що виконують керівні та координуючі ролі, від оптимального визначення компетенції яких суттєво залежить ця безпека в масштабах усієї держави.

У цілому в структурі державної системи забезпечення інформаційної безпеки можна виокремити чотири основні владні підсистеми, більш відомі як гілки влади, які, в свою чергу, мають різні функцій у сфері забезпечення такої безпеки і, відповідно, неоднакову компетенцію:

1) президент України;

2) законодавча влада;

3) виконавча влада;

4) судова влада.

Особливістю реалізації функції забезпечення інформаційної безпеки є те, що кожен із цих органів:

– працює, використовуючи інформаційну інфраструктуру суспільства;

– продукує і споживає інформаційні ресурси;

– установлює відповідні відносини з громадянами як представник власника державних інформаційних ресурсів і складових інформаційної інфраструктури;

– має здійснювати певні дії для збереження цих ресурсів і забезпечення безпеки функціонування інформаційних і телекомунікаційних систем, мереж зв’язку та систем автоматизації управління.

У політики щодо інформаційної безпеки (так само, як і в будь-якої іншої політики) є власні принципи:

– принцип дотримання Конституції і законодавства України, всесвітньо визнаних принципів і норм міжнародного права;

– принцип відкритості у реалізації функцій органів державної влади, до якого належить інформування суспільства про їх діяльність, ураховуючи обмеження, встановлені законодавством;

– принцип правової рівності всіх, хто бере участь в інформаційній взаємодії, незалежно від їх політичного, соціального, економічного тощо статусу;

– принцип пріоритетного розвитку вітчизняних сучасних інформаційних і телекомунікаційних технологій [8; 159; 247].

Відповідно, найважливішими завданнями держави із забезпечення цієї безпеки є такі:

– забезпечення передбачених Конституцією прав і свобод громадян України в розглядуваній сфері;

– удосконалення української інформаційної інфраструктури та її захист; інтеграція України до світового інформаційного простору;

– протидія загрозі протиборства в інформаційній сфері [8; 159; 246; 248].

Отже, реалізовуючи свої функції в розглядуваній сфері, держава:

– об’єктивно і всебічно аналізує та прогнозує загрози інформаційній безпеці України, вживає заходів щодо її убезпечення (зокрема, розробляє нові);

– організовує роботу законодавчих і виконавчих органів державної влади з реалізації заходів, спрямованих на запобігання, усунення та нейтралізацію загроз інформаційній безпеці держави;

– підтримує і координує діяльність ГО щодо об’єктивного інформування населення про різноманітні соціально важливі явища, забезпечує захист суспільства від викривленої та недостовірної інформації;

– контролює розроблення, створення, розвиток, використання, експорт та імпорт засобів захисту інформації шляхом їх сертифікації та ліцензування діяльності у відповідній галузі;

– реалізує необхідну протекціоністську політику щодо виробників засобів інформатизації і захисту інформації на території України і вживає заходів щодо захисту внутрішнього ринку від проникнення на нього неякісних таких засобів та продуктів;

– сприяє наданню доступу різним особам (як юридичним, так і фізичним) до світових інформаційних ресурсів і глобальних інформаційних мереж;

– розробляє і втілює в життя державну інформаційну політику;

– розробляє державні програми щодо забезпечення розглядуваної безпеки, об'єднуючи для цього відповідні зусилля державних і недержавних організацій;

– допомагає інтернаціоналізації глобальних інформаційних мереж і систем, а також входженню України у світове інформаційне співтовариство як рівноправного партнера [8; 159; 246; 248].

\

4.3. Удосконалення державної системи інформаційної безпеки

Регіональний інформаційно-психологічний простір – це багатовимірна мережа, побудована з прямих і зворотних зв'язків суб'єктів інформаційних взаємодій регіону, які є середовищем реалізації інформаційно-психологічних впливів. При цьому суб'єкт такого впливу необхідно визначити як активну складову цього процесу, здатну впливати на інші складові за допомогою виконання якихось дій. Об'єктом інформаційно-психологічного впливу є пасивна складова цього процесу, що перебуває під згаданим впливом будь-якого суб'єкта. Інформаційно-психологічним впливом в цьому випадку вважається дія (процес), що викликає зміни інформаційно-психологічних властивостей об'єкта (системи), та забезпечує переведення його в якісно

новий стан. Предмет такого впливу − це властивість, притаманна цьому об'єкту (системі), яка змінюється під час здійснення інформаційно-психологічного впливу на цей об'єкт [110; 111; 141].

У зв'язку зі специфікою сфери інформаційно-психологічних впливів, в ній об'єкт одного впливу водночас є суб'єктом іншого. Визначаючи об'єкт та предмет забезпечення інформаційно-психологічної безпеки слід ураховувати, що наразі основним правовим актом, покликаним окреслити межі безпечного стану як індивідуальної, так і групової (чи масової) свідомості, є Конституція України [110].

Об'єкти інформаційно-психологічних впливів можна класифікувати так:

1) житель регіону як громадянин − суб'єкт суспільно-політичного життя (носій світогляду, володар правосвідомості і менталітету, духовних ідеалів і ціннісних установок, типових для цього регіону);

2) житель регіону як особистість − індивід, що має свідомість, схильний до інформаційних впливів, результати яких можуть прямо загрожувати його фізичному чи психічному здоров'ю;

3) групи і маси людей − сукупності людей, що мають якусь спільну ознаку (національну, релігійну, професійну, родинну тощо), або об'єднаних лише спільним територіальним перебуванням (населення регіону, натовп тощо) [110; 141].

Предмети інформаційно-психологічного впливу можна згрупувати в такі класи:

– конституційні права і свободи людини і громадянина;

– гідність особи;

– фізичне і психічне здоров'я жителів, адекватне сприйняття ними дійсності;

– моральні цінності і культурна спадщина;

– територіальна та ін. спільність жителів [110; 111; 141].

Чинниками, що впливають на таку безпеку в межах конкретного регіону, вважаються умови, що формуються в системі (в цьому випадку в соціумі), які не є безпосередніми загрозами інформаційно-психологічній безпеці, але сприяють появі цих загроз.

До чинників, що безпосередньо впливають на цю безпеку окремих громадян, груп, масових об'єднань чи населення в цілому, можна віднести:

– економічні (інфляція, підвищення тарифів на комунальні послуги, явне та приховане безробіття, майнове розшарування);

– соціальні (погіршення ефективності системи освіти і виховання під час формування масової культури; зростання депопуляції населення, злочинності, алкоголізму і наркоманії, зростання міжетнічної напруженості, деструктивна роль нетрадиційних релігійних конфесій, поширення ісламського фундаменталізму і релігійного сектантізму);

– політичні (недостатнє інформування про політику влади, нерозвиненість методів і засобів протидії негативним інформаційно-психологічним впливам);

– науково-технічні (інформатизація, поява нових способів, методів і засобів впливу на свідомість, зокрема нових технологій ЗМІ, комп'ютерних технологій тощо) [106; 109; 111].

Метою інформаційно-психологічного впливу є очікувана, запланована зміна властивостей людини або соціуму. При цьому типові цілі як в регіональному, так і в міжнародному масштабі можна поділити на групи так:

– підпорядкування індивіда або регіонального соціуму (переорієнтація переваг особи або громадської думки в інтересах суб'єкта, що чинить вплив), прикладом цього можуть служити вибори в органи влади, у процесі яких цілеспрямована корекція думки виборців завжди проводиться тим або іншим кандидатом; для індивіда прикладом такого інформаційно-психологічного впливу може служити гіпноз тощо;

– дезорганізація функціонування індивіда або регіонального соціуму (дезорієнтація особистості або руйнування соціальної організації при

масових інформаційно-психологічних впливах); прикладом тому можуть служити численні факти інформаційно-психологічного впливу на суперника в змаганні (спортивному, політичному тощо) і виведення його зі стану стійкої психічної рівноваги, у разі масових таких впливів спроби дезорганізації соціуму зазвичай робляться опозиційними деструктивними силами;

– знищення індивіда або групи (ударний інформаційно-психологічний вплив призводить до самоліквідації індивіда або групи людей), прикладом можуть служити терористи-смертники або груповий суїцид на релігійному ґрунті – в обох випадках інформаційно-психологічний вплив знищує один з базових інстинктів людини − інстинкт самозбереження, підміняючи його фанатичним догмами [4; 15; 36; 58; 68; 115; 156; 228].

Засобами таких впливів є матеріальні предмети та фізичні поля, за допомогою яких працюють:

– ЗМІ (теле-, радіо компанії і друковані органи, листівки, плакати, предмети повсякденного вжитку);

– віртуально-психологічні засоби (комп'ютерні іграшки, Інтернет-сайти тощо);

– спеціальні технічні засоби.

Застосування цих засобів іде шляхом приховування, викривлення інформації та її знищення.

Джерелами загроз інформаційно-психологічній безпеці виявляються самі суб'єкти, їхні дії та процеси, що при цьому відбуваються, які призводять до виникнення загроз. Зокрема, для регіону до них можна віднести:

– діяльність іноземних і вітчизняних економічних, політичних, військових, розвідувальних та інформаційних структур (зокрема, недобросовісна конкуренція);

– діяльність терористичних організацій на території регіону;

– криміногенну обстановку в регіоні;

– агітаційну діяльність ГО, політичних партій, кандидатів у політичні лідери, що спотворює інформаційний простір регіону;

– антиконституційна діяльність неформальних релігійних, етнічних та інших об’єднань [94].

Загальним принципом виявлення цих загроз повинна бути можливість аналізованих чинників стати джерелом потенційної небезпеки для реалізації конституційних норм, присвячених гарантіям прав і свобод. Тому на ці конституційні гарантії накладають такі два обмеження:

1) заборона пропаганди або агітації, що розпалюють соціальну, расову, національну чи релігійну ненависть і ворожнечу, а також пропаганди соціальної, расової, національної, релігійної, мовної тощо переваги одних груп перед іншими;

2) обмеження конституційних прав і свобод громадян законодавством у тих випадках, коли це необхідно для захисту основ конституційного ладу, здоров’я, прав та законних інтересів громадян, а також для оборони країни та забезпечення державної безпеки.

Можна виділити такі головні чинники, через які в країнах Європейського Союзу необхідно створювати і розвивати державну систему інформаційної безпеки та які, відповідно, доцільно враховувати в аналогічній діяльності в Україні:

– реструктуризація управління господарською діяльністю, підвищення самостійності регіонів держави, а також підприємств, установ та організацій, які перебувають на їх території, зокрема у зовнішньоекономічній діяльності;

– зростання рівня залежності результатів діяльності органів державної влади, місцевого самоврядування, підприємств, установ та організацій від своєчасності отримання використовуваної ними інформації, її достовірності, а також від надійності заходів, ужитих для збереження в таємниці інформації обмеженого доступу;

– надання інформації статусу об’єкта власності, розвиток інформаційних ресурсів, що перебувають у володінні регіонів держави,

підприємств, організацій, установ і громадян, а також необхідність захисту цих ресурсів від протиправних дій;

– збільшення обсягів інформації, що становить будь-яку таємницю (службову, комерційну, професійну, особисту тощо), але при цьому використовується і передається в органах державної влади і місцевого самоврядування; неоднозначність класифікації тієї ж самої інформації під час її обробки в різних державних і недержавних установах; необхідність однакового захисту такої інформації незалежно від місця перебування її носіїв;

– широке використання в органах влади й управління регіональних і глобальних інформаційних систем, які накопичують і передають величезні обсяги цінної інформації, але лишаються при цьому недостатньо захищеними від несанкціонованого доступу до конфіденційної частини цієї інформації, зростання ризику і небезпеки несанкціонованих і ненавмисних дій стосовно інформації в цих системах;

– підвищення рівня небезпеки інформаційних загроз, що з'являються в безпосередній близькості від об'єктів регіону, який слід захищати; складність прогнозування і виявлення цих загроз, оцінювання їх небезпечності та вжиття адекватних заходів, необхідних для їх усунення;

– формування в державі та її регіонах недержавних структур, до діяльності яких належить інформаційна безпека; широке використання кримінальними структурами пристроїв негласного отримання інформації, зростання кількості пов'язаних з комп'ютерною інформацію злочинів;

– нездатність більшості регіональних підприємств, організацій та установ самостійно організувати ефективний захист інформації внаслідок відсутності фахівців, необхідної нормативно-методичної літератури, високої вартості сертифікованих засобів і послуг, пов'язаних з інформаційною безпекою, пропонованих комерційними організаціями, які є монополістами в цій сфері [183];

– непередбачуваність економічних і соціальних наслідків виникнення критичних ситуацій, спричинених порушеннями безпеки інформації в кредитно-фінансових установах, системах управління екологічно небезпечними виробництвами, транспортом та енергетикою;

– проблема тероризму, що створює очевидну напруженість в регіональному інформаційно-психологічному просторі;

– антиконституційна діяльність неформальних релігійних, етнічних й інших організацій, що чинять деструктивні інформаційно-психологічні впливи на індивідуальну і групову свідомість жителів регіону;

– недобросовісні передвиборчі технології, що викривляють регіональний інформаційний простір і знижують рівень довіри до органів державної влади й органів місцевого самоврядування [159; 246; 248].

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, а також об'єктні (цільові) та функціональні підсистеми державної системи інформаційної безпеки.

Загальними цілями побудови державної системи інформаційної безпеки є такі:

1) провадження державної політики щодо інформаційної безпеки в усій державі та в регіонах, що передбачає вдосконалення її організаційно-правового, нормативно-методичного, технічного та кадрового забезпечення в органах державної влади і місцевого самоврядування, на підприємствах, в установах та організаціях державного та регіонального рівня, в першу чергу позавідомчої приналежності;

2) координація дій державних і недержавних структур певного регіону із захисту відповідного інформаційного простору; створення необхідної інфраструктури для організаційно-правового, нормативно-методичного,

технічного тощо забезпечення такої безпеки в усій державі та в регіонах [246; 248].

Реалізацію першої мети державної системи інформаційної безпеки, перш за все, спрямовано на забезпечення державних інтересів у розглядуваній сфері на рівні конкретного регіону. При цьому необхідно забезпечувати захист найважливішої інформації, що перебуває в розпорядженні органів регіонального управління, та захист усього регіонального інформаційно-психологічного простору.

Реалізацію другої мети зосереджено на соціально-економічній безпеці держави та регіонів. Її досягнення цієї мети вимагає розроблення нових узгоджених механізмів забезпечення інформаційної безпеки, налагодження взаємодії між регіональними і державними органами, що належать до системи її державного забезпечення, та структурами, які працюють у відповідній сфері, на рівні як держави, так і її регіонів [248].

Для досягнення цілей державної системи інформаційної безпеки необхідно створювати і вдосконалювати механізм забезпечення такої безпеки, який охоплює:

– органи вказаної державної системи, які забезпечують виконання всієї повноти завдань і функцій у розглядуваній сфері, та наділяються відповідними повноваженнями;

– систему планових законодавчих, організаційно-розпорядчих, нормативних й інформаційних документів, що врегульовують діяльність органів згаданої державної системи та сприяють її діяльності в інші способи;

– технології, системи і засоби, що перебувають у віданні органів цієї системи [159; 248].

У підґрунті формування державної системи інформаційної безпеки перебувають такі принципи:

– законність;

– розмежування повноважень, пов’язаних із забезпеченням такої безпеки, між державними органами й органами місцевого самоврядування, що належать до державної системи захисту інформації;

– добровільність входження до складу цієї державної системи підприємств, установ та організацій;

– колегіальність керівництва державної системи інформаційної безпеки;

– стабільність ядра цієї системи, завдяки якому і виконуються функції інформаційної безпеки;

– адаптивність оболонки державної системи інформаційної безпеки до зовнішніх умов і завдань;

– раціональне поєднання універсальності та диференціації механізмів забезпечення такої безпеки;

– урахування досвіду її забезпечення по всій Україні та в її регіонах;

– поетапність розбудови і вдосконалення розглядуваної державної системи [8; 133; 159; 248].

Охарактеризуємо їх дещо детальніше. Так, принцип законності полягає в такому:

– створенні державної системи інформаційної безпеки в суворій відповідності до законодавства у цій сфері;

– формуванні системи регіональних нормативно-правових актів, що забезпечує більш ефективне й продумане використання відповідних ресурсів кожного конкретного регіону;

– реалізації правового механізму захисту регіонального інформаційного простору [91; 93; 133; 143; 158; 169; 170; 194; 273; 325].

Принцип розмежування повноважень, пов’язаних із забезпеченням інформаційної безпеки, між державними органами й органами місцевого самоврядування, що належать до державної системи захисту інформації, означає, що на державному рівні визначаються загальні вимоги до забезпечення цієї безпеки, закріплені в системі державних нормативно-

правових документах (зокрема, організаційно-розпорядчого спрямування); на регіональному рівні створюються умови для реалізації цих вимог і механізму, що дозволяє в регіоні успішно протистояти загрозам та уникати заподіяння шкоди інтересам особи, суспільства й держави в розглядуваній сфері.

Принцип добровільності ґрунтується на взаємному отриманні регіональними підприємствами, установами та організаціями вигоди від об'єднання зусиль у вирішенні питань інформаційної безпеки та відсутності втручання державних органів у межі компетенції конкретних власників інформації та інформаційних систем.

Принцип колегіальності керівництва передбачає ухвалення узгоджених рішень з питань безпеки інформації, вигідних для всіх суб'єктів її забезпечення, із повною самостійністю і персональною відповідальністю цих суб'єктів у конкретній галузі діяльності.

Принцип стабільності ядра розглядуваної державної системи передбачає обов'язкову наявність у її складі елементів, які забезпечують пріоритетне виконання функцій інформаційної безпеки у разі реалізації будь-яких варіантів розвитку цієї системи.

Сутністю принципу адаптивності оболонки державної системи інформаційної безпеки є можливість створення відповідно до поточних зовнішніх умов і вирішуваних завдань, гнучкої системи організації діяльності у розглядуваній сфері.

Принцип раціонального поєднання універсальності та диференціації механізмів інформаційної безпеки полягає у визначенні загального механізму її забезпечення і поширенні набутого досвіду, а також у визначенні специфічних вимог і розробленні спеціальних механізмів захисту регіонального інформаційного простору.

Принцип урахування досвіду забезпечення такої безпеки в державі в цілому та в її окремих регіонах проявляється у створенні системи взаємного

обміну інформацією між регіонами, узагальненні та періодичному доведення такого досвіду до відома органів державної системи інформаційної безпеки.

Принцип поетапності розбудови і вдосконалення розглядуваної державної системи реалізується у вигляді визначення цілей і завдань її розвитку, пріоритетності необхідних результатів і раціональної послідовності їх досягнення, що спирається на знання науково-технічних і економічних можливостей держави та регіонів.

Як відомо, джерело і напрямки розвитку будь-якого явища слід шукати в системі суперечностей, що існують в сукупності відносин цього явища з рештою явищ і процесів. Не є винятком і система інформаційного забезпечення державної безпеки в умовах інформаційного суспільства. Тому всі суперечності такої безпеки соціуму умовно можна поділити на три групи, що мають чіткі межі та специфічні способи вирішення [91; 159; 324].

До першої групи слід включити суперечності інформаційної безпеки соціуму як самостійного автономного явища, що має власні особливості та специфічну логіку розвитку. Серед них найбільш чітко вирізняються суперечності структурно-змістовного плану, які утворюють суперечності між рівнями, видами і формами інформаційної безпеки. Водночас суперечності видового порядку, що проявляються в розбіжностях комп'ютерної, культурно-когнітивної й інформаційно-психологічної безпеки, у міру розвитку утворюють свій комплекс суперечностей.

Другу групу утворюють суперечності інформаційної безпеки, що стосуються умов існування та розвитку відповідної сфери соціуму. У цьому випадку виділяються зв'язки інформаційної безпеки з інформаційними відносинами й інформаційною практикою соціальних суб'єктів і з рештою елементів цієї сфери [159].

Третю групу складають суперечності, що сформувалися в результаті відносин інформаційної безпеки з іншими видами безпеки та загальною безпекою соціуму. Досліджуючи цю групу суперечностей, необхідно зрозуміти причини їх розвитку й ураховувати як внутрішні суперечності,

властиві цьому конкретному явищу, так і внутрішні суперечності більш великої системи, які по відношенню до досліджуваного явища виступають як зовнішні та є складною частиною умов виникнення суперечностей. Через це слід спочатку встановити суперечності, що утворилися в результаті зв'язку інформаційної безпеки з рівнями і формами безпеки соціуму та з властивими її системі процесами та явищами. У цьому контексті особливу методологічну цінність мають суперечності між інформаційною безпекою і домінантою безпеки суспільної свідомості.

Проте перелік суперечностей системи інформаційного забезпечення державної безпеки соціуму в умовах цифрового суспільства буде далеко не повним, якщо з поля зору випадуть суперечності функціонування інформаційної безпеки, насамперед суперечності між особистим, громадським і державним рівнями функціонування. Наразі суперечності сходяться на різних рівнях функціонування цієї безпеки, відповідно, на цих рівнях – особистому, громадському і державному – необхідно і говорити про ефективність інформаційної безпеки соціуму та визначати принципово нові проблеми, що потребують інтенсивного інтелектуального опрацювання [248; 269].

Враховуючи зазначені протиріччя, доцільною видається побудова дієвої державної системи інформаційної безпеки, якій притаманні такі властивості, як багаторівневість і багатофункціональність (рис. 4.5).

Ясна річ, що і найповніший, на погляд конкретного дослідника, перелік суперечностей, не охоплює всіх суперечностей системи інформаційної безпеки соціуму, оскільки останні є багатшими, складнішими, різнохарактерними та набагато змістовнішими за будь-які суто теоретичні міркування.

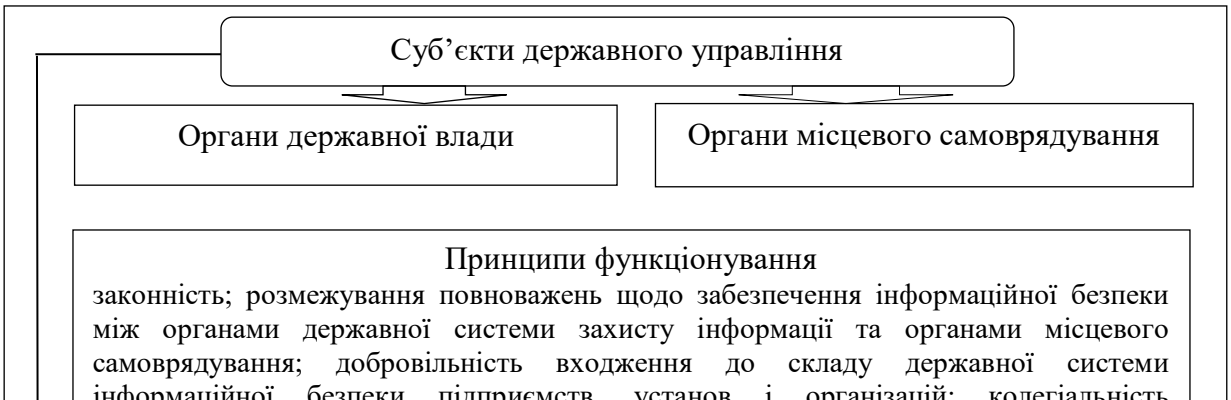

Рис. 4.5. Складові державної системи інформаційної безпеки
Джерело: авторська розробка

Між тим, з усього різноманіття суперечностей системи інформаційного забезпечення державної безпеки соціуму в умовах цифрового суспільства легко виокремлюються найбільш характерні риси, ознаки та базові суперечності, які виступають своєрідним стрижнем всієї сукупності

суперечностей інформаційної безпеки соціуму. Якщо здійснити системний аналіз виділених трьох груп суперечностей інформаційної безпеки соціуму, то можна виявити два домінуючих суперечності, які лежать у підґрунті еволюції цієї системи соціуму.

Перша суперечність пов'язується безпосередньо зі взаємодією основних компонентів системи інформаційної безпеки, як-то «технологія», «небезпека (загроза)» і «захист». В якомусь сенсі вони збігаються, в процесі розвитку переходять один в одного, але в інших − чітко суперечать одне одному.

Іншою головною суперечністю розвитку інформаційної безпеки соціуму є суперечність між життєвою потребою інформаційної сфери в безпечному існуванні та прогресивним розвитком і потенційними можливостями, закладеними внаслідок низки суб'єктивних та об'єктивних обставин на певному етапі історичного розвитку безпосередньо в саму систему такої безпеки. Ця потреба інформаційної сфери знаходить своє практичне втілення в інформаційній практиці соціуму в формі загального соціально-технологічного замовлення [248; 269].

У цілому в процесі роботи із суперечностями інформаційної безпеки соціуму важливо розглядати й усвідомлювати динаміку глобальних інформаційних процесів, темпи наростання конфронтаційних явищ і вплив стримуючих чинників, використання яких може сприяти віддаленню безпосередньої інформаційної небезпеки, а також дасть час для пошуків оптимальних рішень.

Слід відмітити, що провідними напрямками діяльності держави щодо забезпечення інформаційної безпеки регіону є такі:

– формування державних і регіональних інформаційних ресурсів, їх накопичення та раціональне управління ними;

– своєчасне встановлення загроз цій безпеці та їх джерел;

– дотримання пов'язаних з інформацією прав особи, суспільства й органів державної влади та місцевого самоврядування, їх захист від

шкідливих інформаційних впливів (налагодження такого інформаційного обміну із зовнішнім середовищем, який не становить небезпеку для суб'єктів регіону та зовнішнього відносно цього регіону середовища);

– захист інформації обмеженого доступу (яка відповідно до законодавства вважається державною чи службовою таємницею), від ризику її потрапляння до недружніх суб'єктів, серед іншого в результаті здійснення незаконної технічної розвідки та/або несанкціонованого доступу до неї;

– захист від небезпек, породжуваних несанкціонованими і ненавмисними діями, будь-якої іншої інформації незалежно від категорії доступу до неї та/або форми її існування [121; 159; 229; 248].

При цьому першою з проблем, пов'язаних із формуванням регіональних систем інформаційної безпеки, зазвичай стає пошук найкращого співвідношення між командними (директивними) та координаційними методами держуправління. Обмежитись самим лише командним методом у цьому разі неможливо через те, що інформація обмеженого доступу зазвичай циркулює у межах цілої низки установ та організацій і підприємств різних форм власності та різного підпорядкування, що працюють на території цього регіону [121; 229]. До них належать як місцеві органи виконавчої влади й органи місцевого самоврядування, так і інституції зовсім іншого типу – військові частини, науково-дослідні інститути, промислові підприємства (пов'язані з обороною) тощо. Через це комплексі заходи, в яких нерідко повинні бути задіяні кілька власників або користувачів інформації, неможливо реалізувати саме командними методами. Натомість внаслідок частої необхідності об'єднувати зусилля згаданих різних суб'єктів постає питання щодо пошуку чи розроблення і запровадження якогось єдиного, спільного підходу до організації та практичного забезпечення такої безпеки. Суттєвий внесок у вирішення цього питання може внести затвердження єдиної методології оцінювання можливостей реалізації загроз і засобів протидії їм, що має враховувати серед іншого

вплив згаданих засобів захисту інформації на стан усього інформаційного простору в регіоні.

У зв'язку з цим мало не найголовнішим завданням щодо розбудови чи вдосконалення розглядуваних регіональних систем держуправління в цій сфері є досягнення раціонального поєднання командних і координаційних методів. Щоб впоратись із ним має не лише існувати, а й ефективно працювати в регіоні спеціальний координуючий орган, до якого мають увійти всі зацікавлені особи. У свою чергу, згаданим особам повинні делегуватися певні повноваження [121; 229].

Водночас існує і інша проблема, пов'язана із так званими супутніми загрозами безпеці інформації. Ідеться про такі загрози, які можуть проявитися вже в процесі забезпечення інформаційної безпеки і які під час проєктування та заснування системи захисту ще не існували або не були помічені, тож, і не враховувалися. На практиці це зазвичай виявляється як зменшення розмір, такі, яких раніше не існувало, канали витоку інформації. це вимагає передбачення в системі держуправління інформаційною безпекою двох режимів – «повсякденного» й «оперативного».

При цьому в разі застосування основного, повсякденного режиму (він використовується тоді, коли стан системи й об'єкта захисту, а також і загрози безпеці є сталими, незмінними) система управляється за допомогою завчасно розроблених і перевірених на практиці довгострокових програм і планів з відповідними алгоритмами, протоколами та/або інструкціями, при чому використовуються також заздалегідь підібрані, найоптимальніші для конкретних умов технічні й організаційних засоби захисту інформації [101; 180; 248; 268].

У разі переходу до оперативного режиму головним завданням держуправління такою безпекою стає оперативне, швидке встановлення можливих загроз безпеці інформації, їх оцінювання та підготовка рекомендацій з їх запобігання або нейтралізації їх наслідків [248; 269].

Інакше кажучи, другим завданням з удосконалення підсистеми держуправління регіональними системами інформаційної безпеки є підвищення її адаптивності до зовнішніх умов на випадок їх зміни.

Третя проблема держуправління регіональними системами інформаційної безпеки є наслідком неоднаковості та різної приналежності сил і засобів захисту, із сукупності яких на практиці і складаються ці місцеві системи. Зазначена обставина вимагає постійного контролю стану системи й оцінювання її реальних можливостей щодо поведінки в умовах як. Умовно кажучи, звичайних, фонових (таких, що існують постійно), так і нових загроз [248], адже без цього будь-яка, навіть найелементарніша й тимчасова, втрата конкретного одиничного засобу захисту інформації (вихід певного елементу з лад, зокрема і внаслідок регламентних робіт) ризикує призвести до витоку інформації з непередбачуваними наслідками. Із цього випливає, що третім завданням щодо вдосконалення розглядуваної підсистеми має стати постійне, неперервне відстежування стану всіх елементів системи захисту й обґрунтування пропозицій щодо вжиття заходів, що дозволять уникнути появи чи мінімізувати негативні наслідки зміни цього стану. Щоб виконати це завдання на практиці, необхідно здійснювати моніторинг стану регіональних систем інформаційної безпеки щодо певного набору параметрів. При цьому складання переліку останніх є окремим і досить непростим завданням.

Як регіональна система інформаційної безпеки є невід’ємною від такої загальнодержавної системи, так і її система управління співвідноситься із системою управління відповідною державною системою [121]. У зв’язку з цим на початку формування розглядуваних регіональних систем і розгортання такої ж державної системи управління має узгоджуватись за схемою «узгодження входів-виходів», а згодом на основі спільного математичного забезпечення.

Підбиваючи підсумок зазначеному, зауважимо, що в цілому можуть застосовуватися такі методи держуправління цими системами:

– командні (директивні) методи управління, що спираються на організаційно-розпорядчі акти органів виконавчої влади, які зводяться до надання директив щодо виконання ухвалених рішень у розглядуваній сфері;

– метод регламентування відносин у галузі інформаційної безпеки на рівні регіону, основою якого виступає розроблення системи необхідних і достатніх правил і норм, що втілюється у вигляді відповідних правових і нормативних документів;

– низка методів, що ґрунтуються на переконанні, спираючись на доведення й демонстрацію переваг тих методичних рекомендацій, які надаються органами виконавчої влади;

– управління розвитком розглядуваних регіональних систем шляхом обґрунтування пріоритетних напрямків, розроблення і реалізації цільових державних програм розвитку таких систем [59; 100; 121; 229].

Наразі досліджено низку основних функції управління регіональними системами інформаційної безпеки.

Під час реалізації єдиної державної політики у цій сфері мають забезпечуватися:

– збір, систематизація та узагальнення інформації про стан процесів інформаційної безпеки на об’єктах управління; оцінювання стану цієї безпеки в регіоні, виявлення невирішених проблем, передання необхідної інформації про її стан на державний рівень;

– контроль стану інформаційної безпеки на об’єктах управління;

– визначення провідних напрямів забезпечення цієї безпеки на рівні регіону;

– розроблення цільових програм щодо її забезпечення та контроль за їх виконанням;

– організація та/або стимулювання науково-технічних досліджень, присвячених забезпеченню інформаційної безпеки в регіоні; виконання вимог нормативних документів щодо цієї безпеки;

– розроблення та затвердження регіональних нормативних і методичних документів з цієї тематики (концепцій, положень, вимог, норм, моделей, методик, рекомендацій, інструкцій та інших документів);

– надання підприємствам, установам та організаціям методичної допомоги щодо підготовки до ліцензування, в наданні послуг у цій сфері і пов'язаній із цим діяльності, створенні засобів інформаційної безпеки й засобів технічного контролю їх ефективності;

– здійснення методичного управління підготовкою, професійною перепідготовкою та підвищенням кваліфікації фахівців у розглядуваній сфері;

– методичне управління діяльністю органів місцевого самоврядування щодо розбудови муніципальних систем такої безпеки [59; 121; 229].

Під час здійснення координації та функціонального регулювання діяльності із забезпечення інформаційної безпеки необхідно:

– створювати й розвивати організаційно-технічний механізму захисту інформаційного простору регіонів України;

– забезпечити на плановій основі міжгалузеву координацію діяльності щодо забезпечення такої безпеки в апаратах органів державної влади, місцевого самоврядування, на підприємствах, в установах та організаціях шляхом регулярного обговорення Комісією з інформаційної безпеки спільних проблемних питань і ухвалення щодо них узгоджених рішень;

– здійснення методичного управління у розглядуваній сфері щодо апаратів органів державної влади та інших перелічених вище суб'єктів шляхом забезпечення видання, поширення і впровадження в практичну діяльність концепцій, положень, вимог, норм, моделей, методик, рекомендацій, інструкцій та інших документів з інформаційної безпеки;

– сприяння міжрегіональному співробітництву у цій сфері.

Отже, принциповими особливостями управління регіональними системами інформаційної безпеки є такі:

– по-перше, таке управління здійснюється в межах державної системи інформаційної безпеки;

– по-друге, як основні методи управління використовуються координація та функціональне регулювання діяльності із забезпечення такої безпеки;

– по-третє, найважливішим завданням управління її регіональними системами є створення і розвиток механізмів забезпечення цієї безпеки в межах компетенції регіонів України [121; 229].

У цілому завдання щодо вдосконалення управління регіональними системами інформаційної безпеки обумовлюються тим, що всі вище згадані методи управління мають спиратися на об’єктивну, повну і своєчасно отримувану інформацію про процеси, які відбуваються в розглядуваних системах, та передбачати ухвалення достатньою мірою обґрунтованих рішень, що випливатимуть із такої інформації.

У будь-якому разі результати вдосконалення систем інформаційної безпеки треба оцінювати на обох рівнях – і державному, і на регіональному.

Найчастіше як критерії уразливості використовують ймовірність успіху дестабілізуючого впливу, або математичне очікування обсягу збитку. Втім, через розширення кола завдань, які належать зараз до цій сфери, доречно було б уточнити і розвинути похід до формування цих показників [94; 310].

Крім уже традиційних проблем захисту інформації та захисту від інформаційного впливу, в нашій країні дедалі актуальнішою стає проблема створення інформаційного ресурсу, необхідного і достатнього для безпечного функціонування об’єкта (особи, підприємства, міста, області). Найгостріше ця проблема постала в територіальних органах влади (адміністрації регіонів, органи місцевого самоврядування), в яких із кожним днем посилюється залежність якості та безпеки управлінських рішень від особливостей інформаційно-аналітичного забезпечення процесів управління [13; 162; 184].

На підставі вищевикладеного пропонується враховувати як один із критеріїв забезпечення інформаційної безпеки об’єкта (території) відповідність обсягів інформації, потрібної для управління об’єктом, та об’єктивно істинної інформації про його стан.

Для того щоб визначити показники, критерії та методики оцінювання стану регіональної системи інформаційної безпеки, варто виокремити основні елементи цієї системи й визначити їх напрямки діяльності та функції. Оцінювання ефективності й якості виконання функцій окремими елементами системи з урахуванням взаємозв’язків цих функцій дозволить вийти на показники оцінювання стану такої регіональної системи в цілому [94].

Оцінюванням стану регіональної системи інформаційної безпеки вважається процедура визначення показників, які описують поточний стан системи, а також міру виконання системою покладених на неї функцій. Цими функціями, зокрема, є такі:

– процес забезпечення інформаційної безпеки в об’єктних підсистемах;

– загальносистемне забезпечення цілісності та стабільного функціонування регіональної системи такої безпеки в функціональних підсистемах;

– загальносистемне управління її регіональною системою [94].

При цьому функціональні системи регіональної системи інформаційної безпеки являють собою специфічні системи масового обслуговування. На вхід цих систем надходить потік завдань (вимог щось проконтролювати, заявок на ліцензування, сертифікацію, атестацію, надання послуг або проведення робіт зі створення техніки інформаційної безпеки), з якими треба впоратись протягом визначеного часу. Для вирішення завдань використовується певна кількість органів регіональних систем інформаційної безпеки, утворених каналами обслуговування. У зв’язку зі сказаним вище для прогнозування показників стану функціональних підсистем розглядуваних регіональних систем на перспективу доцільно використовувати апарат теорії масового обслуговування.

Показниками оцінювання стану функціональних підсистем таких систем можуть виступати:

– імовірність повного завантаження всіх каналів;

– середній час обслуговування заявки;

– середній час очікування виконання заявки;

– коефіцієнт простою обслуговуючих каналів.

Для розрахунку зазначених показників необхідно описати такі характеристики підсистем:

– вхідний потік, тобто потік вступників вимог або заявок на обслуговування;

– механізм обслуговування;

– дисципліну черги [94; 310].

Зокрема, для опису вхідного потоку слід задати імовірнісний закон, що управляє послідовністю моментів надходження вимог на обслуговування.

Механізм обслуговування характеризується, в першу чергу, тривалістю процедур обслуговування. Тривалість інтервалу часу, необхідного для реалізації процедури обслуговування, частково залежить від запитів клієнта, а частково − від стану самої обслуговуючої системи. Для опису механізму обслуговування треба також вказати кількість і взаємне розташування обслуговуючих приладів або каналів для кожної підсистеми, що досліджується.

Така характеристика, як дисципліна черги, визначає порядок обслуговування вимог, що надходять на вхід системи. Залежно від підсистеми, що моделюється, дисципліна черги може будуватися за схемою типу «першим прийшов − першим обслуговується», може бути випадковим або може формуватися за деякою системою пріоритетів.

Зауважимо, що під час аналізу систем масового обслуговування в більшості випадків практикується застосування такого підходу. Для наближеного опису реальної системи використовуються прості аналітичні моделі. Потім, маючи в своєму розпорядженні результати аналізу вихідних

моделей і, використовуючи ці результати як орієнтир, розробляється імітаційна модель, яка дозволяє врахувати ті аспекти завдання, які, будучи істотними, водночас важко піддаються аналізу на першому етапі моделювання.

Наявні відмінності одних підсистем від інших в структурі та порядку функціонування слід ураховувати шляхом подальшого статистичного імітаційного моделювання цих підсистем.

Певною мірою виконання функцій забезпечення інформаційної безпеки, захисту інформації й управління останнім є характерним для різних рівнів ієрархії регіональної системи інформаційної безпеки. На конкретному підприємстві (в організації) для таких систем найважливішою є функція захисту інформації, однак в інтересах її реалізації виконуються і інші функції. На більш високих рівнях ієрархії регіональної системи інформаційної безпеки великого значення набувають функції управління, координації діяльності та забезпечення захисту інформації.

Стан регіональної системи інформаційної безпеки оцінюється послідовно, починаючи з нижнього рівня ієрархії за окремими підсистемами, з узагальненням результатів оцінювання на вищому рівні [121]. Відповідно, доцільно розглянути систему показників оцінювання стану регіональних систем інформаційної безпеки. Зокрема, воно охоплює:

– оцінювання стану забезпечення інформаційної безпеки на об’єктах захисту;

– оцінювання стану його функціональних підсистем;

– оцінювання стану системи управління такою безпекою.

Зокрема, як індикатор оцінювання стану забезпечення інформаційної безпеки на окремому одиничному об’єкті захисту пропонується використовувати векторний показник, що характеризує виконання або невиконання на ньому встановлених вимог до забезпечення інформаційної безпеки [94; 137].

Такі вимоги містять у собі:

– вимоги до організації процесу забезпечення такої безпеки на об’єкті, зокрема ті, що стосуються всебічного (матеріально-технічного, нормативно-методичного, інформаційного, фінансового тощо) забезпечення цього процесу на об’єкті;

– вимоги до ефективності забезпечення інформаційної безпеки на об’єкті в тій чи іншій стадії його життєвого циклу.

Конкретний зміст вимог визначається на основі чинних нормативних документів, присвячених інформаційній безпеці, з поправками на специфіку конкретного об’єкта захисту.

Для спрощення розрахунків можна вважати, що вимоги забезпечення інформаційної безпеки на об’єкті захисту не виконуються, якщо не виконується хоча б одна з окремих вимог.

Для сукупності об’єктів захисту окремого підприємства та регіональної системи інформаційної безпеки в цілому стан забезпечення такої безпеки оцінюється часткою об’єктів (від загальної кількості об’єктів захисту), на яких виконуються встановлені вимоги. При цьому також повинна враховуватися важливість (категорія) інформації, що підлягає захисту.

Під час вибору показників оцінювання стану функціональних підсистем забезпечення інформаційної безпеки (контролю, атестування, підготовки фахівців тощо) треба враховувати, що ці підсистеми є своєрідними системами масового обслуговування, які відпрацьовують певний потік заявок (вимог) по контролю, атестуванню, підготовці фахівців, створенню техніки забезпечення цієї безпеки задля забезпечення процесу захисту інформації на різних об’єктах захисту. Ефективність таких систем оцінюється за:

– їх пропускною спроможністю;

– імовірністю обслуговування заявок (або за часткою заявок, які обслуговуються);

– часом обслуговування заявки;

– середнім часом очікування заявки в черзі;

– ступенем завантаження або простою елементів систем [310].

До найбільш загальних показників, що відбивають мету функціонування підсистеми, належить ймовірність обслуговування заявок (або частка обслужених заявок від необхідної кількості за певний період часу). Фактичні значення цього показника визначають на підставі статистичних даних про результати роботи підсистем. Крім того, функціональні підсистеми можуть характеризуватися показниками оперативності реагування на потреби, що виникають, і якості виконання функцій покладених на ці підсистеми. Для оцінювання прогнозних значень показників ефективності та оперативності можна застосовувати добре опрацьовані аналітичні й імітаційні моделі масового обслуговування. Якість виконання функцій підсистеми визначається за встановленим набором вимог до підсистеми, що характеризують її якість. До таких вимог, зокрема, можуть належати:

– обґрунтованість ухвалених рішень при атестуванні об’єктів і контролі стану забезпечення інформаційної безпеки;

– рівень підготовки фахівців;

– рівень надаваних послуг тощо [310].

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.

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 [121]. 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 [121; 229].

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 [94].

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 [48; 310].

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 [48].

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) [310]. 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 [229]. 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) [248; 250; 275].

Висновки до четвертого розділу

1. Підкреслено необхідність вироблення ефективної комплексної внутрішньої і зовнішньої державної інформаційної політики як інструменту регулювання взаємодій усіх компонентів відповідного соціуму, виходячи з національних інтересів держави та необхідності збереження територіальної цілісності та суверенітету України.

2. Виділено принципові особливості процесу розроблення та реалізації єдиної державної політики у сфері інформаційної безпеки: вона формується в межах державної системи забезпечення такої безпеки. Головними методами управління у зазначеному контексті виступають координація та функціональне регулювання діяльності із забезпечення інформаційної безпеки. Найважливішим завданням розроблення та реалізації єдиної державної політики у розглядуваній сфері є створення і розвиток механізмів забезпечення такої безпеки у межах компетенції органів державної влади та місцевого самоврядування.

3. Запропоновано поділити всі суперечності інформаційної безпеки соціуму відповідно до специфічних шляхів їх вирішення на три умовні групи, кожна з яких має чіткі межі.

До першої групи мають увійти суперечності інформаційної безпеки соціуму як самостійного автономного явища, що має власні особливості та специфічну логіку розвитку. Серед них найбільш чітко вирізняються суперечності структурно-змістовного плану, які утворюють суперечності між рівнями, видами і формами інформаційної безпеки. Водночас суперечності видового порядку, що проявляються в розбіжностях комп'ютерної, культурно-когнітивної й інформаційно-психологічної безпеки, у міру розвитку утворюють свій комплекс суперечностей.

Другу групу утворюють суперечності інформаційної безпеки, що стосуються умов існування та розвитку відповідної сфери соціуму. У цьому випадку виділяються зв'язки інформаційної безпеки з інформаційними відносинами й інформаційною практикою соціальних суб'єктів і з рештою елементів цієї сфери [1].

Третю групу складають суперечності, що сформувалися в результаті відносин інформаційної безпеки з іншими видами безпеки та загальною безпекою соціуму. Досліджуючи цю групу суперечностей, необхідно зрозуміти причини їх розвитку й ураховувати як внутрішні суперечності,

властиві цьому конкретному явищу, так і внутрішні суперечності більш великої системи, які по відношенню до досліджуваного явища виступають як зовнішні та є складною частиною умов виникнення суперечностей. Через це слід спочатку встановити суперечності, що утворилися в результаті зв'язку інформаційної безпеки з рівнями і формами безпеки соціуму та з властивими її системі процесами та явищами.

4. 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, а також об'єктні (цільові) та функціональні підсистеми державної системи інформаційної безпеки.

5. Зазначено, що у підґрунтя формування державної системи інформаційної безпеки можуть бути покладені такі принципи: законність; розмежування повноважень, пов'язаних із забезпеченням такої безпеки, між державними органами й органами місцевого самоврядування, що належать до державної системи захисту інформації; добровільність входження до складу цієї державної системи підприємств, установ та організацій; колегіальність керівництва державної системи інформаційної безпеки; стабільність ядра цієї системи, завдяки якому і виконуються функції інформаційної безпеки; адаптивність оболонки державної системи інформаційної безпеки до зовнішніх умов і завдань; раціональне поєднання універсальності та диференціації механізмів забезпечення такої безпеки; врахування досвіду її забезпечення по всій Україні та в її регіонах; поетапність розбудови і вдосконалення розглядуваної державної системи.

6. Показано, що існує можливість застосування таких методів держуправління регіональними системами інформаційної безпеки:

– командні (директивні) методи управління, що спираються на організаційно-розпорядчі акти органів виконавчої влади, які зводяться до надання директив щодо виконання ухвалених рішень у розглядуваній сфері;

– метод регламентування відносин у галузі інформаційної безпеки на рівні регіону, основою якого виступає розроблення системи необхідних і достатніх правил і норм, що втілюється у вигляді відповідних правових і нормативних документів;

– низка методів, що ґрунтуються на переконанні, спираючись на доведення й демонстрацію переваг тих методичних рекомендацій, які надаються органами виконавчої влади;

– управління розвитком розглядуваних регіональних систем шляхом обґрунтування пріоритетних напрямків, розроблення і реалізації цільових державних програм розвитку таких систем.

7. 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.

РОЗДІЛ 5. ШЛЯХИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ ТА ЗАГРОЗ

5.1. Концептуальні положення інформаційного забезпечення державної безпеки

Розроблення Концепції інформаційного забезпечення державної безпеки України доречно починати з визначення самого ключового поняття «інформаційне забезпечення державної безпеки». Краще за все розуміти під ним сукупність тісно пов’язаних між собою заходів правового, організаційного, оперативно-розшукового, розвідувального, контррозвідувального, науково-технічного, інформаційно-аналітичного, кадрового, економічного тощо характеру щодо забезпечення заходів із виявлення, прогнозування, запобігання, стримування і нейтралізації інформаційних загроз та ліквідації їх наслідків для держбезпеки у разі їх реалізації [103; 228].

Практично Концепція інформаційного забезпечення держбезпеки відображає множину узятих разом офіційних поглядів на сутність і зміст діяльності України щодо вказаного забезпечення та захисту держбезпеки від внутрішніх і зовнішніх загроз. Ця Концепція визначає завдання, пріоритети, напрями та очікувані результати у сфері інформаційної безпеки особи, суспільства і держави і сприяє конструктивній взаємодії між органами державної влади різних рівнів, бізнесом та різними громадськими об’єднаннями для захисту національних інтересів України в інформаційній сфері. Також ця Концепція покликана забезпечити єдність підходів до формування та реалізації відповідної державної політики щодо інформаційної безпеки й виступити методологічним підґрунтям для розроблення та вдосконалення присвячених їй нормативно-правових актів.

На основі цього засадничого документу формується відповідна державна політика й розвиваються суспільні відносини у розглядуваній сфері, а також розробляються і втілюються в практичну площину заходи з удосконалення української системи забезпечення інформаційної безпеки.

Зростаючий ступінь відкритості економік, свободи переміщення товарів, капіталів і трудових ресурсів та міжособистісної взаємодії розмиває кордони між внутрішніми і зовнішніми політичними, економічними й інформаційними процесами.

Технологічна еволюція стає джерелом принципово нових загроз і нових різновидів негативного впливу на особу, суспільство та державу. Нині посилюється роль і вплив ЗМІ та глобальних комунікаційних механізмів. Інформаційні технології знайшли широке застосування в управлінні найважливішими об’єктами життєзабезпечення, які стають більш вразливими перед випадковими і навмисними діями.

Відповідно, Концепція інформаційного забезпечення державної безпеки визначає основні стратегічні цілі, завдання та напрями, які держава має реалізувати для забезпечення її інформаційної безпеки.

Процес поступального розвитку України як суверенної і процвітаючої держави неможливо розглядати поза контекстом наявних загальносвітових тенденцій і реалій. Людство вступило в стадію кардинальних соціальних, політичних, економічних та інших змін, що характеризуються швидким розвитком інформаційної сфери. Останній, у свою чергу, перетворюється на один з визначальних чинників впливу на людей, соціуми і країни.

Провідні держави світу вступили в еру інформаційного суспільства, яке ґрунтується на нових технологіях, методах і нових підходах, або перебувають в процесі його розбудови. У кінцевому підсумку їх використання повинно сприяти:

– адекватній новим реаліям реалізації конституційних прав громадян;

– поліпшенню добробуту населення;

– підвищенню конкурентоспроможності компаній;

– зміцненню державності.

Державним органам це нове суспільство надає можливість ефективніше надавати послуги громадянам, покращити діяльність державного апарату і підвищити рівень довіри громадян до держави. Завдяки цьому від ступеню розвиненості інформаційного суспільства прямо залежить процес функціонування державних інститутів, отже, він впливає на економіку й обороноздатність кожної країни. У реаліях сучасного світу наявність адекватного потребам громадян інформаційного суспільства стало запорукою загальної спроможності держави.

Істотну проблему становить поширення інформаційної злочинності (кіберзлочинності), серед іншого діяльність організованих транснаціональних злочинних груп. Специфіка кіберзлочинів полягає в їх вельми високій латентності, тобто кількість офіційно зареєстрованих злочинів, учинених з використанням сучасних інформаційно-комунікаційних технологій, становить лише невеликий відсоток від реально скоєних. Боротьба з інформаційною злочинністю вимагає від правоохоронних органів і спецслужб адекватного оперативного реагування на неї шляхом проведення спільних скоординованих дій з аналогічними спеціальними службами та правоохоронними органами зарубіжних країн [45; 140; 226; 243; 269].

Незважаючи на те, що цей вид злочинності не став настільки поширеним на території України, наразі його динаміка характеризується такими рисами:

– стійкою тенденцією зростання використання телекомунікаційних технологій;

– витонченістю;

– появою нових способів вчинення злочинів, доведення яких сильно утруднено через відсутність необхідних правових, організаційних тощо інструментів [243].

Відповідно, назріла необхідність вироблення нових концептуальних заходів протидії злочинам і правопорушенням у сфері інформаційних технологій, що ґрунтуються на:

– постійному оновленні нормативно-правової бази;

– здійсненні технічного переозброєння;

– широкому залученні громадськості;

– пошуку нових форм і методів протидії згаданим негативним явищам.

Посилюється роль і вплив глобальних ЗМІ та комунікаційних механізмів на економічну, політичну, соціальну тощо ситуацію в різних країнах. Фундаментальні зміни, що сталися останнім часом у державах з різними економічними і політичними умовами, вказують на ключову роль у цих процесах нових технологій управління масами, серед іншого за допомогою соціальних мереж, використання масової розсилки стислих повідомлень за допомогою мобільних телефонів і спеціальних сайтів тощо. Широке використання населенням України соціальних мереж і блогів створює можливість їх використання для надання цілеспрямованого впливу на внутрішньополітичну ситуацію на шкоду національним інтересам держави [20; 163; 165; 224].

Негативним проявом відкритості національного інформаційного простору і зростання популярності зарубіжних ЗМІ, зокрема телебачення та інтернет-ресурсів (поштових служб, соціальних мереж, блогів і відеопорталів) є поява реальної загрози інформаційного впливу на громадську думку і свідомість населення. Інформаційний вплив може виражатися як у вигляді прямого нав’язування ідей, здатних заподіяти шкоду національним інтересам України, так і у вигляді створення певного інформаційного тла, яке штучно підтримується шляхом маніпулювання інформацією або її тенденційним коментуванням. Для протидії такому маніпулюванню суспільною свідомістю треба:

– серйозно поліпшити якість державної інформаційної політики;

– підвищити відкритість державних органів;

– краще забезпечувати права громадян на інформацію.

Серйозні загрози містить у собі проблема неконкурентоспроможності вітчизняного контенту. Його якість залишається недостатньою для повноцінної конкуренції з іноземним інформаційним і розважальним продуктом. В умовах відкритості національного інформаційного простору це призводить до його низької популярності. У свою чергу, низька популярність не дозволяє залучити значні інвестиції в його виробництво, що призводить до крайньої недостатності виробництва вітчизняного контенту.

Відсутність інформаційних технологій, що відповідають потребам вітчизняних держави, бізнесу і суспільства, змушує використовувати іноземні обладнання й інформаційні системи. Через це збільшується загроза несанкціонованого доступу до інформації, включно з тією, яка вимагає підвищеного захисту, водночас розвивається залежність держави від іноземних виробників комп'ютерної та телекомунікаційної техніки і програмного забезпечення [269].

Перевірки захисту державних баз даних, включених до складу «електронного уряду», свідчать про відсутність адекватного правового, організаційного й технічного режиму захисту персональних даних громадян. Відсутність відповідних механізмів створює передумови для зловживання персональними даними в кримінальних цілях, зокрема:

– підробки документів;

– шахрайства;

– незаконного копіювання і поширення різних баз даних.

На жаль, доводиться констатувати, що в Україні система захисту інформації функціонує недостатньо ефективно, серед іншого недостатньою мірою використовуються технічні засоби її захисту від несанкціонованого доступу і копіювання. Не повною мірою реалізуються політика безпеки й організаційно-технічні заходи, які протидіють витоку інформації, наслідком чого стають зловживання повноваженнями в корисливих цілях. Втрати важливої інформації призводять до:

– безсистемності захисту даних і слабкій координації відповідних заходів у загальнодержавному масштабі;

– відомчої роз'єднаності в забезпеченні цілісності й конфіденційності інформації.

Дедалі гостріше постає проблема браку кваліфікованих кадрів в інформаційно-комунікаційної сфері, серед іншого і в сфері інформаційної безпеки [93].

Наразі є необхідним подальше вдосконалення процесів і підходів до навчання й підвищення кваліфікації фахівців різних державних інституцій, діяльність яких пов'язано із захистом державних секретів і забезпеченням інформаційної безпеки.

Певну загрозу становить порівняно низький рівень в українському суспільстві загальної правової інформаційної культури, зокрема навичок безпечного використання кіберпростору.

Істотно відстає від потреб поточного дня правове забезпечення розглядуваної сфери [23; 148; 325]. Недостатньо розроблено і самі правові механізми регулювання інформаційних правовідносин, які складаються під час пошуку, надходження і використання інформації й різних інформаційних ресурсів, продуктів і послуг [252]. Потребують поліпшення і актуалізації правові механізми, що регулюють процеси створення, передання і поширення інформації та пов'язаних із нею відповідних ресурсів, продуктів і послуг. Найбільшу проблему становить регулювання інформаційних правовідносин, що стосуються формування та використання інформаційних систем і їх мереж, телекомунікаційної інфраструктури тощо [78; 124; 153; 186; 220; 251; 327].

Крім того, стан правового забезпечення протидії інформаційним злочинам наразі характеризується також:

– недостатньою узгодженістю наявних правових механізмів у цій сфері;

– фрагментарністю діяльності суб'єктів законодавчої ініціативи, що стосується згаданих вище правових механізмів;

– недостатньою ефективністю та суперечливістю правових норм;

– недосконалістю правової статистики.

Вищевказані проблеми в правовому забезпеченні інформаційної сфери створюють серйозну загрозу інформаційній безпеці держави. Це доводить нагальну необхідність виділення в Україні окремої галузі законодавства − інформаційного права [78; 157; 186; 327].

Останнім часом актуалізується проблема рівноправної участі нашої держави в міжнародному обміні інформацією і в процесах міжнародного регулювання інформаційної безпеки. Необхідність обстоювання національних інтересів України вимагає підвищення активності державних органів в межах діяльності існуючих міжнародних організацій [160; 178].

Таким чином, поточний стан забезпечення інформаційної безпеки в Україні в сучасних умовах характеризується такими загрозами:

– недосконалість системи забезпечення цієї безпеки і порушення функціонування життєво важливих елементів інформатизації;

– низький рівень виробництва, впровадження та використання сучасних інформаційно-комунікаційних технологій, що не відповідає об’єктивним потребам суспільства;

– залежність України від імпорту інформаційних технологій, програмного забезпечення, засобів інформатизації та захисту інформації тощо, потенційно шкідливих для наших національних інтересів;

– загострення інформаційного протиборства між провідними світовими центрами сили, підготовки і ведення закордонними державами боротьби в інформаційному просторі;

– неконструктивна політика іноземних держав у сфері глобального інформаційного моніторингу, циркуляції інформації та нових інформаційних технологій;

– розвиток технологій маніпулювання інформацією;

– можливості шкідливого для наших національних інтересів інформаційного впливу на суспільну свідомість і державні інститути;

– поширення недостовірної або навмисне викривленої інформації, потенційно шкідливої для наших національних інтересів;

– відкритість для зовнішнього впливу і уразливість національного інфопростору;

– недостатня ефективність інформаційного забезпечення державної політики;

– слабка захищеність і низька конкурентоспроможність національного інфопростору;

– невідповідність якості національного контенту об'єктивним потребам суспільства і світовому рівню;

– зростання злочинності, серед іншого транснаціональної, а також та екстремістської і терористичної діяльності, в якій використовуються інформаційно-комунікаційні технології;

– спроби отримати ззовні несанкціонований доступ до інформаційних ресурсів України, що призводять до заподіяння шкоди її національним інтересам;

– шкідлива для інтересів України діяльність іноземних розвідувальних і спеціальних служб, іноземних політичних та економічних структур;

– порушення режиму секретності під час роботи з відомостями, що становлять державні секрети України, а також навмисні неправомірні дії та ненавмисні помилки і порушення під час роботи з інформацією обмеженого доступу;

– недостатній розвиток системи правового регулювання цієї сфери;

– стихійні лиха і катастрофи;

– неправомірні дії державних структур, що порушують законні права та інтереси фізичних і юридичних осіб та держави в розглядуваній сфері [80; 113; 230; 262].

До головних національних інтересів України в інформаційній сфері належать такі:

– забезпечення дотримання конституційних прав громадян, що стосуються інформації;

– формування і поступальний розвиток інформаційного суспільства;

– рівноправна участь держави у світовому інформаційному обміні;

– формування, функціонування та захист єдиного національного інфопростору;

– випереджаючий розвиток інформаційно-комунікаційних технологій;

– ефективне та своєчасне інформаційне забезпечення органів державної влади;

– недопущення фактів втрат і розголошення інформації з обмеженим доступом до неї, а також іншої захищеної інформації;

– досягнення надійного та стійкого функціонування життєво важливих інформаційних систем і ресурсів та пов'язаної із ними інфраструктури.

У результаті розквіту в Україні процесів інформатизації суспільства і держави, зокрема випереджальної розбудови «електронного уряду», склалися передумови для побудови інформаційного суспільства, водночас розвиток вищевказаних процесів призвів до посилення наявних і появи нових проблем і небезпек в інформаційній сфері [231; 247; 259; 319].

У міждержавних відносинах посилюється тенденція використання інформаційного тиску як дієвого механізму глобальної конкуренції. Використання різних засобів інформаційної війни й інформаційної експансії стало важливим, навіть майже невід'ємним інструментом вирішення великих конфліктів політичного, соціального, економічного тощо характеру. Активно використовується методи блокування Інтернет-ЗМІ шляхом проведення розподілених комп'ютерних атак [316; 366]. Більшість розвинених країн вже створили в складі своїх збройних сил інформаційні війська і не приховують намірів їх активного використання [74; 142].

Великі держави, які здатні здійснювати глобальний моніторинг поширюваної інформації, використовують його результати для отримання

однобічних переваг у міждержавних відносинах (політичних, економічних, військових, екологічних тощо).

Екстремістські й терористичні організації і групи дедалі активніше використовують можливості глобальних інформаційно-комунікаційних мереж для пропаганди своєї ідеології, вербування та навчання однодумців, підтримки зв'язку і фінансування різних терористичних груп. Поширення різнохарактерних радикальних ідей серед молоді України викликає заклопотаність. Відзначаються випадки, коли громадяни України під впливом цілеспрямованої пропаганди, серед іншого за допомогою Інтернету, беруть участь у незаконних акціях в різних регіонах світу. Зростає загроза здійснення комп'ютерних атак на інформаційні системи держави як методу терористичної діяльності. Такі атаки вже неодноразово були зафіксовані в багатьох країнах [52].

Відповідно, метою Концепції інформаційного забезпечення державної безпеки є формування такої державної системи її забезпечення, яка гарантуватиме захист національних інтересів України в цій сфері.

Досягнення цієї мети вимагає вирішення комплексу таких завдань:

– розвиток системи управління інформаційною безпекою, що дозволяє забезпечити захищеність відповідної національної інфраструктури та єдиного національного інфопростору;

– розроблення і реалізація єдиної державної політики у розглядуваній сфері, зокрема розвиток і зміцнення національної системи захисту інформації;

– забезпечення захисту прав та інтересів особи, суспільства і держави в цій сфері;

– формування вітчизняного інфопростору;

– удосконалення законодавства, що регламентує цю сферу;

– активізація міжнародне співробітництва у вигляді участі нашої держави у процесах формування і використання глобальних інформаційних мереж і систем.

Ефективність реалізації цієї Концепції залежить від рівня консолідації зусиль зацікавлених державних органів, бізнесових структур, ГО та інших організацій громадського суспільства і широкого загалу.

У цілому забезпечити інформаційну безпеку України планується протягом 5 років.

Унаслідок реалізації Концепції інформаційного забезпечення державної безпеки мають бути досягнуті такі цілі:

– удосконалення інформаційних технологій і телекомунікацій;

– недопущення інцидентів, що тягнуть за собою несанкціонований доступ, втрату або викривлення інформації;

– забезпечення щорічної 100 % атестації державних інформаційних систем щодо вимог інформаційної безпеки;

– підвищення затребуваності споживачами вітчизняної інформаційної продукції;

– збільшення частки вітчизняного контенту в ЗМІ;

– скорочення простою інформаційних систем, пов’язаного з безпекою;

– забезпечення виробництва вітчизняного комп’ютерного обладнання, комплектуючих, периферійних пристроїв і програмних продуктів;

– посилення інноваційної активності у промисловості;

– удосконалення нормативно-правової бази щодо інформаційної сфери, серед іншого стосовно міжнародного співробітництва у цій сфері;

– удосконалення системи кадрового забезпечення у сфері інформаційної безпеки і захисту державних секретів.

Реалізація цієї Концепції у кінцевому підсумку допоможе:

– реалізувати громадянам передбачені Основним законом права на отримання, зберігання і поширення повної, достовірної та своєчасної інформації;

– забезпечити рівноправну участь України у світових інформаційних відносинах;

– ефективному інформаційному забезпеченню політики держави;

– забезпечити надійність і стійкість функціонування критично важливих інформаційних систем;

– налагодити безперебійне функціонування і надійний захист єдиного національного інфопростору.

Реалізація завдань Концепції інформаційного забезпечення державної безпеки вимагає розвитку трьох напрямів:

– законодавчого та нормативно-методичного;

– організаційно-розпорядчого й організаційно-технічного;

– кадрового.

Зокрема, у напрямі законодавчого та нормативно-методичного забезпечення треба вирішувати питання розвитку партнерства держави і суспільства з координації зусиль щодо забезпечення національних у розглядуваній сфері, серед іншого створення моделі взаємодії державного і недержавного секторів з протистояння загрозам інформаційній безпеці на національному рівні, що охоплюватиме:

– протидію інформаційному тероризму й інформаційній злочинності;

– розроблення єдиної державної політики у розглядуваній сфері;

– ухвалення законодавчих та вжиття інституційних заходів з розвитку ЗМІ.

Зокрема, будуть:

– визначені відповідальні органи з вироблення політики інформаційної безпеки країни;

– розмежовані сфери відповідальності державних органів, задіяних у забезпеченні цієї безпеки і захисту державних секретів;

– створені механізми їх ефективної міжвідомчої координації [269].

Крім того, буде визначено перелік критично важливих об’єктів інформатизації (серед іншого інформаційних систем і ресурсів), від яких залежить інформаційна безпека всієї держави [38; 215].

При цьому єдина державна політика у розглядуваній сфері повинна забезпечити розроблення та реалізацію єдиних стандартів стосовно вимог до

інформаційної безпеки в державних і недержавних інформаційних системах і ресурсах та пов'язаній із ними інфраструктурі. Зокрема, необхідно актуалізувати чинні нормативно-правові і технічних актів, що стосуються інформаційно-технічного розвитку та захисту інформації (включно з державною таємницею). Буде проведено:

– градацію інформаційних систем і ресурсів за рівнями інформаційної безпеки;

– удосконалення процедур сертифікації технічних і програмних засобів;

– атестацію інформаційних систем на відповідність вимогам такої безпеки;

– посилення міжнародного співробітництва у цій сфері;

– вироблення державних заходів, покликаних посилити відповідальність за стан інформаційної безпеки і захист державних секретів.

Крім того, реалії сьогодення вимагають:

– виділення наявних норм законодавства в окрему галузь законодавства − інформаційне право [317];

– розроблення законодавства щодо захисту критичної інформаційної інфраструктури;

– внесення змін до чинного законодавство з питань віднесення окремих видів інформаційних правопорушень до кримінально караних діянь;

– додаткової правової регламентації питань дотримання авторського права в інформаційно-комунікаційних мережах;

– удосконалення законодавства, що стосується захисту персональних даних;

– розвитку міжнародних правових норм у сфері інформаційної безпеки і захисту державних секретів для забезпечення національних інтересів України.

Поряд із викладеним, необхідно сформувати єдину нормативно-правову базу, яка дозволить:

– упорядкувати діяльність у сфері телерадіомовлення;

– встановити сучасні єдині стандарти і параметри роботи у сфері ефірного цифрового, кабельного, супутникового та інших видів телерадіомовлення;

– підвищити конкурентоспроможність вітчизняних телевізійних і радіоканалів.

Беручи до уваги транскордонний характер питань забезпечення інформаційної безпеки, потрібне подальше вдосконалення міжнародного співробітництва у цьому напрямі, що ґрунтуватиметься на принципах рівноправного інформаційного обміну між державами [178].

Також необхідно:

– розробити міжнародні правові норми щодо регулювання міждержавних відносини стосовно використання глобальної інформаційної інфраструктури;

– налагодити взаємодію українських правоохоронних органів з іноземними з метою запобігання, встановлення випадків і припинення використання інформаційних і телекомунікаційних технологій у терористичних та інших злочинних цілях, а також ліквідації його наслідків;

– гармонізувати національну систему стандартів і сертифікації у цій сфері з міжнародними стандартами та нормативами.

У напрямі організаційно-розпорядчого й організаційно-технічного забезпечення треба реалізувати комплекс заходів із забезпечення інформаційної безпеки критично важливих об’єктів інформатизації та провадити єдину державну політику в цій сфері, серед іншого щодо системи захисту інформації. Вирішити цю проблему надасть можливість формування єдиної державної системи моніторингу інфопростору, а також розбудова Оперативного центра забезпечення інформаційної безпеки, включно з його інформаційною системою та інфраструктурою [159].

Не менш актуальним є питання інноваційного розвитку у розглядуваній сфері, для чого необхідно створювати умови, сприятливі для інноваційної

діяльності, забезпечення проведення відповідних науково-дослідних і дослідно-конструкторських робіт та виробництва програмних і технічних засобів роботи з інформацією, зокрема її захисту [79].

Також треба:

– удосконалювати єдину інформаційно-комунікаційну мережу державних органів;

– створити Оперативний центр забезпечення інформаційної безпеки для координації зусиль щодо захисту критичної інфраструктури, пов'язаної з інформаційнми технологій;

– створити єдиний шлюз доступу державних органів до Інтернету;

– запровадити для цих органів єдину електронну поштову систему;

– створити щонайменша два територіально рознесені центри зберігання резервних баз даних державних органів;

– розвивати національну систему ідентифікації в кіберпросторі України;

– формувати вузли кібербезпеки;

– підвищувати якість та надійність систем забезпечення інформаційної безпеки «електронного уряду», покликаних не допускати несанкціонований доступ, втрату та викривлення інформації.

Крім того, державні органи мають забезпечити атестування державних інформаційних систем щодо дотримання вимог інформаційної безпеки, і це теж сприятиме зменшенню часу простою інформаційних систем.

Для підвищення частки вітчизняного виробництва теле- і радіопрограм буде продовжена практика реалізації державного інформаційного замовлення з активним залученням державних органів до підготовки тематичних напрямів.

Також для забезпечення доступу громадян до вітчизняного контенту буде вжито заходів для подальшого розвитку національної супутникової мережі, серед іншого в напрямі модернізації телекомунікаційної

інфраструктури та формування переліку теле- і радіоканалів, які розповсюджуються за допомогою супутника.

Критеріями під час відбору теле- і радіоканалів повинні стати показники охоплення:

– наявність власної аудиторії;

– охоплення різних цільових груп;

– якість контенту;

– соціальна значимість;

– тематична диференціація;

– рейтинги;

– наявність власних інформаційних продуктів;

– досвід роботи на ринку;

– кваліфікація штату;

– наявність відповідного обладнання і приміщень тощо.

Цей конкурс стимулюватиме вітчизняні теле- і радіоканали використовувати і поширювати якісний і конкурентоспроможний контент.

Також потрібна реалізація цілеспрямованої політики з виявлення та недопущення прихованого впливу на громадську думку з боку інших держав, транснаціональних корпорацій і різних неформальних структур, серед іншого через соціальні мережі, а також активізація протидії поширенню ідеології тероризму, релігійного й етнічного екстремізму, сепаратизму та інших антигромадських проявів за допомогою систем поширення масової інформації [85; 217].

Буде також впроваджено:

– оптимальну модель розвитку і регулювання українського сегмента мережі Інтернет;

– вироблення механізмів стимулювання виробництва позитивного змістовного контенту;

– розвиток вітчизняних інтернет-ЗМІ;

– модернізація телекомунікаційної інфраструктури.

Реалізація цих заходів спрямована на посилення присутності українських ЗМІ в європейському і міжнародному інформаційному просторі для формування позитивного іміджу країни.

Крім того, розвиватиметься міжнародне співробітництво щодо проведення дослідницьких проєктів у межах найперспективніших напрямів науки, технологій і техніки.

У галузі кадрового забезпечення треба вирішити питання вдосконалення системи підготовки фахівців із забезпечення інформаційної безпеки і захисту державних секретів, а також кадрового забезпечення підрозділів правоохоронних органів, серед іншого фахівців з протидії інформаційному тероризму та інформаційній злочинності. Важливим залишається питання підвищення ефективності навчальних та освітніх програм у розглядуваній сфері [93].

Організаційне забезпечення питань реалізації Концепції інформаційного забезпечення державної безпеки пропонується покласти на уповноважені державні органи. Саме ці органи й організації повинні вживати заходів щодо включення відповідних заходів, які випливають із Концепції інформаційного забезпечення державної безпеки, до стратегічних планів і програмних документів [95].

Фінансове та матеріально-технічне забезпечення Концепції інформаційного забезпечення державної безпеки передбачається здійснювати за рахунок і в межах коштів, що виділятимуться на це в загальнодержавному і місцевих бюджетах.

5.2. Стратегічні орієнтири інформаційного забезпечення державної безпеки України

Для сучасної цивілізації нині розпочався новий етап науково-технічної революції, специфічною особливістю якого слугує проникнення в усі сфери життя інформаційно-комунікаційних технологій. Ці технології уже почали

змінювати весь спосіб життя людей. Водночас вони створюють фундамент і матеріальну базу для завершення формування інформаційного суспільства, яке характеризуватиметься якісно новим політичним, соціальним, економічним і культурним розвитком [100; 268].

У світі повсюдно спостерігаються такі тенденції, як:

– трансформація під впливом інформаційно-комунікаційних технологій всіх інститутів суспільства і галузей діяльності;

– прогрес у всіх сферах розроблення, виробництва та використання сучасних технологій;

– прагнення до формування розвиненого інформаційної середовища, адекватного завданням соціально-економічного розвитку країни;

– забезпечення гарантованого рівноправного доступу населення до інформаційних ресурсів;

– спроби підготувати громадян, громадські інститути, бізнес та органи державної влади різних рівнів до існування й роботи в умовах зміненого суспільства.

Перш ніж щось пропонувати стосовно інформаційного забезпечення держбезпеки України, доцільно проаналізувати сучасний стан вітчизняної інформаційної безпеки, зокрема опитати керівників потужних ІТ-компаній, що працюють на території України.

У зв’язку з цим керівникам згаданих компаній було запропоновано відповісти на декілька питань. Перше з яких – «Які механізми повинні використовуватися в державі для підвищення ефективності управління процесами забезпечення інформаційної безпеки?» Узагальнення відповідей на це запитання подано у табл. 3.1.

Із табл. 3.1 можна побачити, що пріоритетним механізмом підвищення ефективності управління процесами забезпечення інформаційної безпеки 27 % респондентів уважають введення засобів безперервного моніторингу контролю доступу. На другому місці перебуває введення засобів управління обліковими записами – 10 %. Однак 45 % опитаних пропонує введення

альтернативних механізмів підвищення ефективності управління згаданими процесами в державі.

Таблиця 3.1

Розподіл відповідей керівників ІТ-компаній України щодо механізмів підвищення ефективності управління процесами забезпечення інформаційної безпеки

Найменування механізму підвищення ефективності	Відсоток розподілу відповідей, %
Введення засобів безперервного моніторингу контролю доступу	27 %
Аутсорсинг окремих заходів у сфері безпеки	4 %
Стандартизація на базі єдиної системи контрольних процедур	9 %
Уведення системи збалансованих показників	5 %
Уведення засобів управління обліковими записами	10 %
Впровадження додаткових засобів забезпечення безпеки	45 %

Джерело: авторська розробка

У табл. 3.2 подано результати розподілу відповідей респондентів щодо засобів контролю за витоком конфіденційної інформації на державному та регіональному рівнях.

З табл. 3.2 видно, що 21 % респондентів уважають, що формулювання конкретних вимог до доступу до конфіденційної інформації є ключовим компонентом засобів контролю за витоком конфіденційної інформації на державному та регіональному рівнях. На другому місці (17 %) перебувають:

– впровадження засобів моніторингу (фільтрації) контенту;

– розроблення та провадження спеціальної політики щодо класифікації конфіденційної інформації.

Таблиця 3.2

Розподіл відповідей керівників ІТ-компаній України щодо розподілу відповідей респондентів стосовно засобів контролю за витоком конфіденційної інформації на державному та регіональному рівнях

Найменування засобу контролю витоку інформації	Відсоток розподілу відповідей, %
Впровадження засобів моніторингу (фільтрації) контенту	17 %
Використання засобів аудиту	6 %
Впровадження засобів аналізу журналу подій	5 %
Обмеження доступу до конфіденційної інформації визначеними періодами часу	9 %
Блокування (обмеження) використання визначених компонентів програмного забезпечення	11 %
Заборона використання пристроїв зі вбудованою камерою в зонах обмеженого доступу	3 %
Розроблення та впровадження спеціальної політики по відношенню до класифікації конфіденційної інформації	17 %
Впровадження додаткових механізмів безпеки з метою захисту інформації	
Обмеження (заборона) застосування систем миттєвого обміну повідомленнями під час передання конфіденційної інформації	11 %
Формулювання конкретних вимог до доступу до	21 %

конфіденційної інформації	

Джерело: авторська розробка

Третє місце (11 %) посідають:

– блокування (обмеження) використання певних компонентів програмного забезпечення;

– обмеження (заборона) застосування систем миттєвого обміну повідомленнями під час передання конфіденційної інформації.

Третє питання, що підлягало дослідженню, – «Які питання повинні розглядатися у державній програмі стосовно підвищення обізнаності стосовно безпеки?» Відповідні результати опитування презентовано у табл. 3.3.

Таблиця 3.3

Розподіл відповідей керівників ІТ-компаній України щодо питань, які повинні розглядатися у державній програм стосовно підвищення обізнаності стосовно безпеки

Зміст питання державної програми	Відсоток розподілу відповідей, %
Підвищення обізнаності з питань забезпечення інформаційної безпеки	33 %
Перевірка, узгодження та дотримання чинних політик і стандартів у сфері безпеки	26 %
Оцінювання ефективності заходів з підвищення рівня обізнаності та вдосконалення наявної програми на основі такої оцінювання	18 %
Регулярне сповіщення про загрози інформаційній безпеці	8 %
Розповсюдження інформаційних повідомлень з нових актуальних тем	7 %
Проведення спеціальних заходів і тренінгів у	8 %

сфері безпеки	

Джерело: авторська розробка

З табл. 3.3 помітно, що підвищення обізнаності з питань забезпечення інформаційної безпеки (33 %) перебуває на першому місці у рейтингу опитаних щодо питань, які повинні розглядатися у державній програмі стосовно підвищення обізнаності стосовно безпеки.

На другому місці перебуває перевірка, узгодження та дотримання чинних політик і стандартів у сфері безпеки (26 %). Третє місце посідає оцінка ефективності заходів з підвищення рівня обізнаності та вдосконалення наявної програми на основі такого оцінювання (18 %).

Наприкінці доцільно проаналізувати відповіді респондентів щодо заходів, які в нинішніх умовах здійснюються державою для мінімізації ризиків інформаційній безпеці (табл. 3.4).

Таблиця 3.4

Розподіл відповідей керівників ІТ-компаній України щодо заходів, які в нинішніх умовах впроваджуються державою для мінімізації ризиків інформаційній безпеці

Зміст заходу	Відсоток розподілу відповідей, %
Оцінювання та вдосконалення засобів контролю за змінами в інформаційних системах	38 %
Оцінювання та вдосконалення засобів управління доступом та обліковими записами	16 %
Впровадження програми попередження витоку даних	33 %
Розроблення програми збереження знань	13 %

Джерело: авторська розробка

З табл. 3.4 можна побачити, що більшість респондентів орієнтується на такі державні заходи мінімізації ризиків інформаційній безпеці:

– оцінювання та вдосконалення засобів контролю за змінами в інформаційних системах (38 %);

– впровадження програми попередження витоку даних (33 %).

Здійснений вище аналіз показує, що провідною є роль у формуванні національної стратегії інформаційного забезпечення держбезпеки у контексті консолідації всіх верств суспільства для досягнення цілей інформаційного й інноваційного розвитку, а також координації бізнесу, всіх суспільних інститутів і громадян щодо реалізації цієї стратегії.

Спираючись на міжнародний досвід формування інформаційного суспільства, в межах Стратегії інформаційного забезпечення державної безпеки можна виокремити чотири ключові напрями:

1) підвищення ефективності системи держуправління;

2) забезпечення доступності інформаційно-комунікаційної інфраструктури;

3) створення інформаційного середовища для подальшого розвитку суспільства у соціально-економічній і культурній сферах;

4) удосконалення українського інформаційного простору.

У межах цих напрямів за допомогою розповсюдження інформаційно-комунікаційних технологій буде вирішено такі завдання:

– удосконалення держуправління;

– створення відкритого і мобільного «електронного уряду»;

– підвищення доступності інформаційної інфраструктури.

Ураховуючи, що розвиток інформаційного суспільства тягне за собою відповідні зміни і людських ресурсів, у Стратегії інформаційного забезпечення державної безпеки необхідно передбачити умови для надання громадянам можливостей опанувати навичками роботи з інформаційними технологіями за допомогою електронної освіти, довічного навчання і професійної підготовки, дистанційної роботи, а також розбудова системи

доступної електронної охорони здоров'я (рис. 5.1). Крім цього, щоб зробити економіку нашої країни відкритішою, доступнішою та більш конкурентоспроможною, у Стратегії інформаційного забезпечення державної безпеки слід передбачити широке впровадження інтелектуальних систем в основні галузі економіки [89; 328].

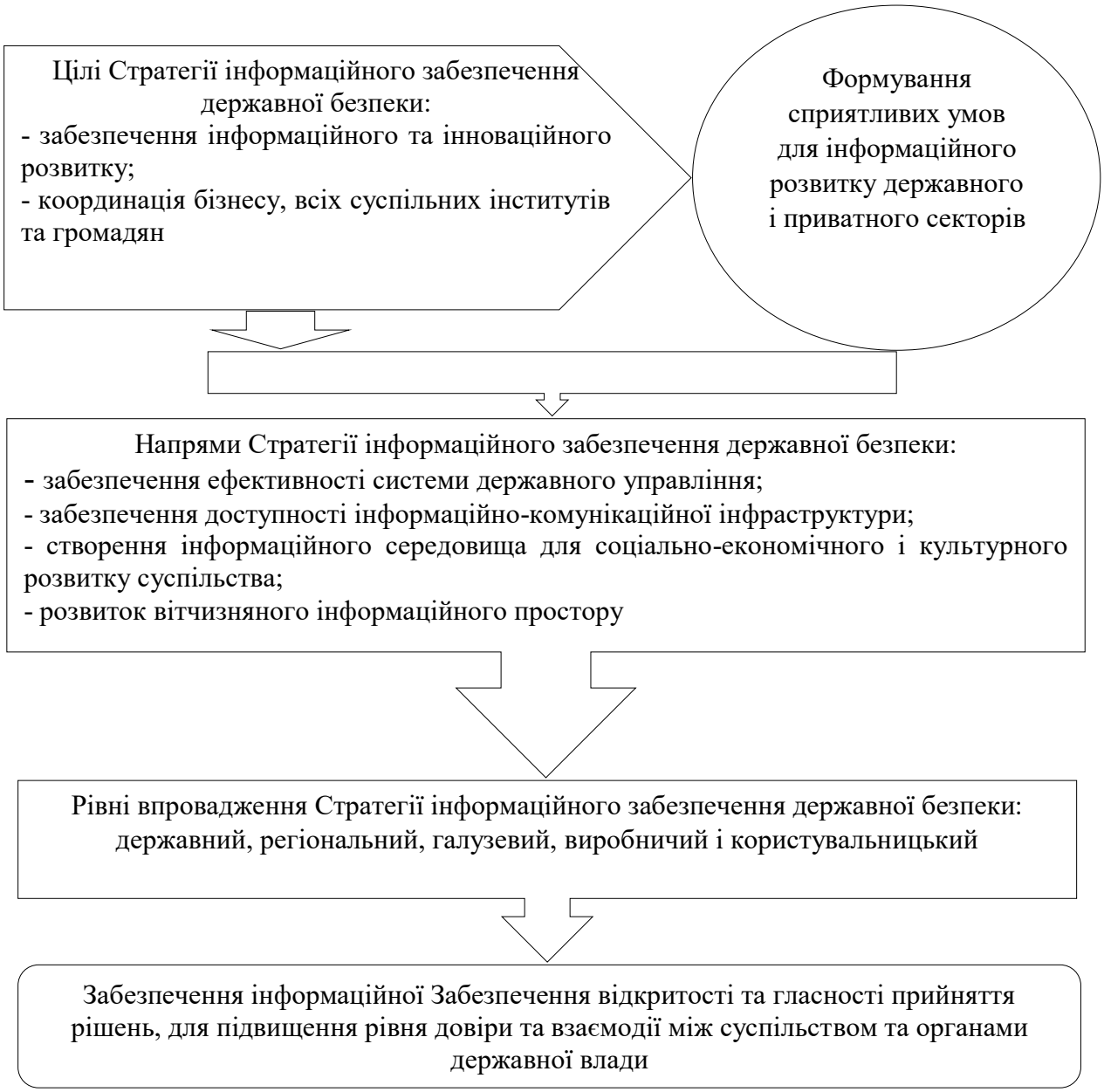

Рис. 5.1. Узагальнена модель формування Стратегії інформаційного забезпечення державної безпеки

Джерело: авторська розробка

Для досягнення ефективності політики переходу до інформаційного суспільства потрібна консолідація зусиль бізнесу і держави у напрямі широкого застосування інформаційно-комунікаційних технологій та надання електронних послуг [100].

Передбачається, що в Україні завершальним етапом реалізації переходу до інформаційного суспільства стане Державна програма «Інформаційна Україна−2030».

Швидкий розвиток інформаційно-комунікаційних технологій і їх адаптація стають важливими чинниками модернізації суспільства, впливаючи не лише на економічні показники, але і на спосіб життя людей, що доводить значущість розвитку цих технологій як для економіки держави, так і для життя громадян [100].

При цьому головними тенденціями сфери телекомунікацій є такі:

– розвиток інфраструктури, що ґрунтується на високошвидкісних оптичних і бездротових технологіях;

– надання мультимедійних послуг населенню та організаціям;

– впровадження і розвиток цифрових технологій телерадіомовлення;

– збільшення рівня цифровізації телефонного зв’язку.

Наразі уже здійснюються заходи з удосконалення дозвільної системи та контрольно-наглядової діяльності державних органів; автоматизується процес видання дозвільних документів; законодавчо закріплено норми щодо спрощення дозвільних процедур, а також впроваджено механізм, що дозволяє встановлювати періодичність перевірок на основі системи управління ризиками інформаційній безпеці.

Усі ці заходи спрямовано на досягнення таких показників:

– скорочення часових витрат і витрат бізнесу;

– зменшення адміністративних бар’єрів;

– упорядкування контрольної діяльності державних органів;

– покращення якості надання населенню державних послуг.

Також реалізується низка заходів, спрямованих на автоматизацію й оптимізацію бізнес-процесів надання державних послуг.

Наразі інформаційні технології вже визнано одним з провідних шляхів створення ефективної системи держуправління. Вони повинні розглядатися як каталізатор та інструмент адміністративних реформ. Застосування на всіх рівнях державних органів інформаційних технологій забезпечить впорядкованість в питаннях контролю, а також виключить дублювання бізнес-процесів і даних, що в підсумку дозволить скоротити витрати бюджетних коштів і покращити якість надаваних населенню послуг [330].

Ефективність роботи державних органів доцільно підвищувати шляхом застосування архітектурного підходу, який передбачає автоматизацію їх діяльності за допомогою створення інформаційно-комунікаційної архітектури для кожного державного органу, узгодженою з уповноваженим органом.

Інформаційно-комунікаційна архітектура державного органу становитиме сукупність документів, моделей, матриць і діаграм, які містять детальний опис поточного й планованого стану державного органу, а також план заходів з оптимізації взаємозалежностей і зв’язків між функціями, бізнес-процесами, даними, інформаційними системами і компонентами технічної інфраструктури у межах плану інформатизації для забезпечення реалізації стратегічних цілей і завдань відповідного органу. Інформаційно-комунікаційна архітектура створюватиметься на основі моделі, яка міститиме такі пов’язані між собою компоненти:

– архітектура діяльності;

– архітектура даних;

– архітектура додатків;

– технологічна архітектура;

– архітектура інформаційної безпеки.

Крім того необхідно сформувати інформаційно-комунікаційну архітектуру органів місцевого самоврядування, яка дозволить уніфікувати діяльність державних органів у регіонах за рахунок використання єдиних бізнес-процесів, шаблонів документів, стандартів і типових рішень в межах інформаційно-комунікаційних технологій.

Передбачається, що ця інформаційно-комунікаційна архітектура буде складатися з трьох рівнів: область, місто та район.

На основі опрацьованої інформаційно-комунікаційної архітектури необхідно розробити детальні документи, що регламентуватимуть бізнес-процеси, які виконуються в державному органі.

Крім того, необхідно впровадити централізацію процесу управління бюджетами в межах схожих інформаційно-комунікаційних технологій та реалізувати більшість проєктів щодо таких технологій на загальнодержавному рівні.

Також необхідно розробити заходи щодо інформатизації всіх державних органів, які стануть частиною їх стратегічних планів. Заходи з інформатизації повинні перевірятися уповноваженим органом на повноту, несуперечність і спрямованість на впровадження оптимізованої інформаційно-комунікаційної архітектури державних органів [245].

З метою повноцінного виконання планів інформатизації в кожному державному органі необхідно розглянути можливість створення організаційної одиниці, що відповідає за його інформатизацію. Цілі та завдання такої організаційної одиниці мають будуть уніфіковані в масштабах країни.

Крім того, необхідно розробити кар’єрну систему для керівників систем інформаційно-комунікаційних технологій державних органів та механізм їх ротації між державними органами та комерційним сектором.

Результати оцінювання якості діяльності державних органів у напрямі впровадження інформаційних технологій мають публікуватися у відкритих джерелах.

При цьому необхідно посилити відповідальність державних органів за порушення регламентів реалізації інформаційно-комунікаційних проєктів забезпечення інформаційної безпеки як ключової частини нацбезпеки.

Ще одним важливим компонентом Стратегії інформаційного забезпечення державної безпеки України є міжнародне співробітництво щодо інформаційної безпеки.

Міжнародне співробітництво у цій сфері є невід'ємною складовою співробітництва в інших важливих сферах – політичній, економічній, військовій. Воно покликано підвищити інформаційну безпеку всіх країн – членів світового співтовариства, включно з Україною.

Провідними напрямами такого співробітництва у розглядуваній сфері, які відповідають інтересам України, є:

1) протидія несанкціонованому доступу до:

а) конфіденційної інформації у міжнародних банківських мережах і каналах інформаційного забезпечення торгівлі по всьому світі;

б) конфіденційної інформації у міжнародних політичних, економічних і військових союзах, блоках та організаціях;

в) інформації в міжнародних правоохоронних організаціях, орієнтованих на боротьбу з міжнародною організованою злочинністю, міжнародним тероризмом, розповсюдженням наркотичних речовин і незаконною торгівлею зброєю;

2) забезпечення інформаційної безпеки під час транскордонного інформаційного обміну та його інформаційного регламенту, а також збереження і забезпечення правдивості інформації під час її передання по національним телекомунікаційним каналам і каналам зв'язку;

3) координація діяльності держав − учасників міжнародного співробітництва із запобігання комп'ютерних злочинів.

Для реалізації зазначених напрямів міжнародного співробітництва у розглядуваній сфері потрібні:

– активна участь України у діяльності всіх міжнародних організацій, що діють у цій сфері;

– обмін досвідом у цій сфері, серед іншого через міжнародні та вітчизняні друковані видання;

– розширення участі українських фахівців у міжнародних конференціях, семінарах і виставках.

Для дослідження методологічних і науково-технічних проблем забезпечення міжнародної інформаційної безпеки бажано створити під егідою ООН міжнародний науково-дослідний інститут.

З урахуванням запропонованої Стратегії інформаційного забезпечення державної безпеки України необхідно розробити основні положення відповідної державної політики в розглядуваній галузі.

Так, головним завданням держави у сфері забезпечення громадської безпеки є забезпечення високої готовності органів правопорядку та екстрених служб до швидкої взаємодії щодо попередження, запобігання та вжиття необхідних заходів із убезпечення життя кожного громадянина України в умовах екстрених ситуацій і стихійних лих будь-якого характеру [158].

Взаємодія органів правопорядку й екстрених служб передбачає насамперед інформаційний обмін і злагоджену роботу всіх їх структур за обставин, що становлять небезпеку для життя і здоров'я. У таких ситуаціях необхідно відзначити особливу роль інформаційно-комп'ютерних технологій, що дозволяють оперативно обмінюватись даними і виступати засобом своєчасного інформування та оповіщення населення про майбутні небезпеки і загрози [194].

Органи правопорядку вживають усіх необхідних заходів з удосконалення механізму охорони громадського порядку і забезпечення безпеки у різноманітних громадських місцях. У зв'язку з цим головним завданням використання в роботі органів правопорядку й екстрених служб сучасних інформаційно-комп'ютерних технологій (далі – ІКТ) є підвищення рівня громадської безпеки та загальної якості роботи цих служб та органів.

Відповідними цільовими індикаторами слід уважати:

– покращення комп'ютерної грамотності працівників екстрених служб;

– скорочення часу реагування на надзвичайні ситуації;

– збільшення частки населених пунктів, оснащених сучасною системою масового оповіщення населення про надзвичайні ситуації [137].

Завдання з підвищення рівня громадської безпеки та ефективності роботи органів правопорядку й екстрених служб шляхом впровадження ІКТ можуть бути виконані шляхом здійснення таких заходів:

– для досягнення більшої ефективності та якості виконання завдань необхідно продовжити роботу з автоматизації операційної та виробничої діяльності екстрених служб;

– продовження роботи з розвитку центрів оперативного управління у всіх регіонах країни для постійного моніторингу вулиць та місць масового скупчення громадян на предмет виявлення підозрілих особистостей, подій, дорожньо-транспортних та інших подій для оперативного реагування на злочини;

– запровадження курсів підвищення комп'ютерної грамотності для працівників екстрених служб з акцентом на вивчення ІКТ, що застосовуються у службовій діяльності;

– продовження роботи у напрямі подальшого розвитку систем своєчасного оповіщення за допомогою всіх засобів зв'язку, включно з мобільними пристроями, для підвищення оперативності запобігання надзвичайних ситуацій та їх ліквідації.

На основі викладених принципів і положень визначаються загальні напрями розроблення і втялення в життя державної інформаційної політики щодо забезпечення безпеки у політичній, військовій тощо сферах.

Державна політика інформаційного забезпечення державної безпеки України як механізм узгодження інтересів суб'єктів інформаційних відносин і пошуку компромісних рішень передбачає формування й організацію ефективної роботи різних робочих груп, комітетів і комісій з широким представництвом фахівців і всіх зацікавлених структур [8; 88; 273].

Нагадаємо, що в контексті переходу суспільства до інформаційного важливим завданням держави є забезпечення небайдужості кожного громадянина до подальшої долі країни, високого рівня громадської солідарності та довіри до влади.

Наразі основні функції щодо забезпечення інформаційного супроводу діяльності держави покладено на уповноважений орган в галузі інформації – Міністерство інформаційної політики України. Однак така практика має низку істотних недоліків, серед яких найбільше вимагають уваги такі:

– розмивання відповідальності за ефективність кінцевого інформаційного продукту;

– існування часового та смислового розриву між фактичною діяльністю та її інформаційним відображенням у ЗМІ.

Поділ питань реалізації та PR-супроводу між державними органами призводить до значного зниження ефективності заходів, покликаних покращувати імідж держави. Уповноважений орган у сфері інформації не завжди володіє повною інформацією і не знайомий з наявною галузевою специфікою, тоді як у решти державних органів немає відповідних повноважень і бюджетів для просування власних досягнень [34; 164].

Між тим, державними органами не повною мірою використовуються можливості нових технологій, внаслідок чого громадяни країни не отримують належного доступу до наявної інформації про діяльність держави.

Відповідно, ключовим завданням політики інформаційного забезпечення держбезпеки є вдосконалення системи координації та підвищення відповідальності державних органів з висвітлення та просування діяльності держави.

У цьому контексті слід виділити відповідні цільові індикатори, якими виступають:

– покращення поінформованості населення про провідні та соціально значущі напрями діяльності держави;

– збільшення частки працівників прес-служб державних органів і національних компаній з відповідною фаховою освітою.

Отже, необхідно окреслити шляхи досягнення виконання зазначених завдань. Так, слід переглянути інформаційну роботу держави з акцентуванням уваги на забезпеченні повноти, своєчасності та достовірності надаваної громадянам інформації. Для цього необхідно об’єднати всю активність щодо інформаційного супроводу держави в єдину державну PR-стратегію, яка зможе замінити численні ситуативні галузеві медіаплани, які просувають окремі аспекти діяльності держави, але сумарно не досягають цілі державної інформаційної політики. Таку PR-стратегію необхідно збалансувати щодо представленості всіх сфер життєдіяльності населення, як-то: освіта, трудова діяльність, охорона здоров’я, надзвичайні ситуації, цивільні права тощо. Водночас слід регулювати інтенсивність застосування в цілому всіма державними органами різних каналів комунікацій і форматів подання даних [164].

Політика інформаційного забезпечення держбезпеки має враховувати інформаційні потреби та бажані канали доступу до інформації громадян всіх категорій і представників ділового співтовариства. Особливу увагу при цьому необхідно приділити представленості державних органів у соціальних майданчиках мережі Інтернет.

Слід також переглянути механізми управління інформаційним простором з чітким розмежуванням компетенцій, сфер відання, повноважень тощо конкретних державних органів та організацій, а також виділити єдиний керівний центр, що визначатиме стратегію у розглядуваній сфері [159].

Новий механізм реалізації політики інформаційного забезпечення держбезпеки доречно відобразити в єдиному алгоритмі міжвідомчої взаємодії, що виключає дублювання функцій і приймає до уваги інформаційну роботу держави в період значущих подій в житті країни. На організаційному рівні це спричинить такі зміни:

– прес-служби державних органів трансформуються в повноцінні PR-підрозділи, що несуть відповідальність за підсумковий інформаційний продукт по своїй галузі, який передбачає своєчасне визначення ключових інформаційних запитів громадськості, оперативне оприлюднення позиції держави на виникаючі питання і конструктивну критику, яка знайшла відображення в публікаціях;

– кошти на PR-супровід державних програм і проєктів будуть передбачені в межах їх же власних бюджетів, особливу увагу при цьому буде приділено використанню нових технологій, серед іншого соціальних медіа, а державне замовлення буде спрямовано на інформаційний супровід найважливіших подій у житті країни, реалізацію національних проєктів.

Так само за допомогою державного замовлення на певну державну інформаційну політику вирішуватимуться соціальні, культурні й освітні завдання загальнонаціонального значення [347].

У цілому державі необхідно буде взяти курс на закріплення пріоритетної ролі інформаційної роботи державних органів, чого можна досягти завдяки планомірній методичній роботі, яка передбачає:

– підвищення оперативності реагування прес-служб на запити ЗМІ та громадськості;

– перегляд структури державного замовлення з урахуванням повсюдного доступу населення до Інтернету та мобільним засобам комунікацій;

– покращення якості інформації і прикладних сервісів державних сайтів;

– сприяння розвитку недержавних служб верифікації новинної і подієвої інформації, що генерується за допомогою засобів масових комунікацій.

Інформування населення про діяльність держави теж забезпечуватиметься шляхом прямої взаємодії державних органів з аудиторією ЗМІ, включно з технологіями краудсорсингу.

Описане вище масштабне перетворення інформаційної діяльності державних органів у межах політики інформаційного забезпечення держбезпеки потребуватиме повноцінної інформаційно-аналітичної підтримки на всіх етапах реалізації. Поступовий перехід українського соціуму у стан інформаційного суспільства виключає ситуативний і формальний підхід до виконання такого завдання [231]. Через це необхідно здійснювати на системній основі заходи за такими напрямами:

– проведення моніторингу й аналізу інформаційного поля;

– налагодження сталої роботи з вивчення, адаптації та впровадження в умовах України успішної зарубіжної практики розроблення і ведення інформаційної політики, ефективних медійних технологій, зокрема Інтернету;

– проведення соціологічних досліджень по вивченню інформаційних потреб і проблемних, форматних та жанрових уподобань населення; розроблення рекомендацій з коригування державної інформаційної політики;

– методичне забезпечення питань провадження згаданої державної політики на підставі аналізу даних ЗМІ, а також аналітичних досліджень у галузі мас-медіа.

Для вирішення проблеми належного технологічного забезпечення бізнес-процесів з моніторингу інфопростору, методичного та аналітичного забезпечення з питань реалізації політики інформаційного забезпечення держбезпеки необхідно внести пропозиції щодо оснащення відповідальних державних структур:

– сучасним телекомунікаційним обладнанням;

– засобами збору і довгострокового зберігання інформації;

– системами обробки текстових, аудіо- й відеозаписів, створеним на основі нових технологій, та іншими елементами матеріально-технічної бази.

У контексті цього завдання необхідно також внести пропозиції щодо запровадження автоматизованої системи моніторингу інформаційного простору, що дозволить підвищити об’єктивність оцінювання інформаційної роботи державних органів із застосуванням єдиного алгоритму до різних даних. Істотну користь принесе можливість прискореної обробки великого масиву даних, що неможливо при використанні традиційних способів, які характеризуються обмеженістю людських можливостей.

У цілому механізми реалізації політики інформаційного забезпечення держбезпеки України мають бути гнучкими і своєчасно відображати зміни в політичному, економічному тощо житті країни [230].

Відповідно, основними положеннями згаданої політики щодо конкретних регіонів України є такі.

Конституційні основи державного устрою країни потребують розвитку і поширення на всі сфери життя і діяльності особи, суспільства і держави, включно зі сферою забезпечення інформаційної безпеки. Остання має стати предметом відповідальності органів державної влади всіх рівнів відповідно до закріпленого в Конституції України розмежування їхніх предметів відання і повноважень.

Розроблення регіональних питань забезпечення інформаційної безпеки має низку особливостей, об’єктивно зумовлених загальною структурою країни.

Інформаційна власність регіонів України є різновидом державної власності. Зокрема, вона містить у собі:

– інформаційну власність органів місцевого самоврядування регіонів України;

– інформаційну власність підприємств і установ, створених або придбаних за рахунок коштів регіонів України;

– культурні цінності народів, що населяють територію регіонів України.

Органи влади та інші державні структури управління регіонів України зобов’язані захищати інформаційне право власності, що перебуває на території об’єктів державної інформаційної власності, розташованих на території суб’єктів такої власності органів місцевого самоврядування та інших юридичних і фізичних осіб.

Суб’єкти господарювання в Україні користуються всією повнотою чинних в Україні інформаційних прав. Зокрема, їм гарантуються:

– рівне право доступу на український ринок інформації та засобів забезпечення інформаційної безпеки незалежно від форми власності;

– право використання для вирішення регіональних державних завдань загальнодержавних інформаційних банків даних з дотриманням встановлених правил забезпечення такої безпеки;

– право проведення самостійної внутрішньої та зовнішньоекономічної діяльності у сфері інформаційної безпеки відповідно до законодавства України (включно з підзаконними нормативно-правовими актами);

– право здійснювати захист своїх інформаційних прав і права інформаційної власності як самостійно, так і шляхом звернення до державних і міжнародних правозахисних органів.

Більш детально проробляти провідні напрямки регіональної політики інформаційного забезпечення держбезпеки України мають органи місцевого самоврядування, враховуючи особливості своїх територій і стану та перспектив розвитку господарської сфери [121].

При цьому правове забезпечення інформаційної безпеки визнається пріоритетним напрямом формування механізмів реалізації відповідної політики щодо держбезпеки України. У нашій державі воно охоплює такі компоненти:

– нормотворчу діяльність щодо створення законодавства, присвяченого суспільним відносинам, що стосуються інформаційної безпеки;

– виконавчу та правозастосовну діяльність щодо виконання органами державної влади, різними юридичними особами та громадянами законодавства у сфері інформації та її захисту й інформатизації.

Зокрема, нормотворча діяльність у сфері забезпечення інформаційної безпеки передбачає:

– оцінювання стану чинного законодавства та розроблення програми його вдосконалення;

– формування організаційно-правових механізмів забезпечення цієї безпеки;

– чітке визначення правового статусу всіх суб’єктів у системі інформаційної безпеки, користувачів інформаційних і телекомунікаційних систем та визначення їх відповідальності за забезпечення цієї безпеки;

– створення організаційно-правового механізму збору й аналізу статистики впливу загроз інформаційній безпеці та їх наслідків щодо всіх видів та/або категорій інформації;

– ухвалення нормативно-правових актів різних рівнів, що регламентуватимуть порядок ліквідації наслідків впливів загроз інформаційній безпеці, а також відновлення порушеного права і ресурсів та реалізації компенсаційних заходів.

Виконавчу і правозастосовну діяльність із забезпечення інформаційної безпеки покликано розробити процедури застосування згаданих вище різнорівневих нормативно-правових актів до суб'єктів, що вчинили злочини і проступки, працюючи із закритою інформацією, та/або порушили регламент інформаційних взаємодій, а також правопорушення з використанням незахищених засобів інформатизації. Крім того, зазначена діяльність передбачає передбачення складів правопорушень у межах різних видів відповідальності (кримінальної, адміністративної, цивільної та дисциплінарної).

Усю діяльність щодо правового забезпечення інформаційної безпеки слід будувати на основі трьох фундаментальних положень права − дотримання законності, забезпечення балансу інтересів окремих суб'єктів і держави та невідворотності покарання.

Зокрема, дотримання законності передбачає наявність законів та інших документально зафіксованих норм та їх застосування й виконання суб'єктами права у розглядуваній сфері.

Забезпечення балансу інтересів громадян, інших суб'єктів інформаційних відносин і держави передбачає пріоритет державних інтересів як загальних інтересів усіх суб'єктів. Орієнтація на свободи, права й інтереси громадян не применшує роль держави в забезпеченні нацбезпеки в цілому і у розглядуваній сфері зокрема.

Невідворотність покарання передбачає відповідну ступінь відповідальності у цій сфері, яка реалізується з урахуванням підвищеної соціальної небезпечності загроз інформаційному середовищу суспільства.

Підкреслимо, що в реалізації механізмів правового забезпечення інформаційної безпеки доводиться спиратися на загальну інформатизацію правової сфери. Через це перелік нагальних заходів з реалізації політики інформаційного забезпечення держбезпеки має передбачати:

– розроблення форм, методів і засобів реалізації політики інформаційного забезпечення держ безпеки України, підготовка рішень органів виконавчої влади та документів, що закріплюють її основні положення;

– формування нормативно-правової бази реалізації цієї політики, включно з визначенням послідовності та порядку розроблення законодавчих та інших нормативно-правових актів і створення механізмів їх практичної реалізації;

– аналіз техніко-економічних параметрів програмно-технічних засобів різного походження, що використовуються для забезпечення інформаційної безпеки, і вибір перспективних напрямів розвитку вітчизняної техніки;

– формування державної науково-технічної програми вдосконалення та розвитку методів і засобів забезпечення розглядуваної безпеки, серед іншого їх використання в українських інформаційних і телекомунікаційних мережах і системах з огляду на майбутнє долучення України до глобальних таких мереж і систем;

– запровадження сертифікації вітчизняних та імпортних засобів інформатизації, які планується придбати для використання в органах державної влади, щодо відповідності вимогам інформаційної безпеки;

– удосконалення організаційної структури вітчизняної системи інформаційної безпеки, серед іншого запровадження єдиного центру координації та регулювання діяльності всіх органів у зазначеній системі;

– розроблення системи економічних і статистичних показників, що відображають якість функціонування розглядуваної системи;

– визначення реальних потреб цієї системи у фахівцях, організація системи їх добору, підготовки і перепідготовки.

У цілому політику інформаційного забезпечення держбезпеки передбачається реалізовувати в два етапи:

– 1 етап − 2020−2024 роки;

– 2 етап − 2025−2030 роки.

На кожному з етапів планується зміна показників, що відображають перебіг реалізації політики інформаційного забезпечення держбезпеки (за роками) та вплив програмних заходів на готовність перейти до інформаційного суспільства.

Так, на першому етапі (2020−2024 роки) планується створити нову інформаційно-комунікаційну архітектуру державних органів, а саме:

– переглянути законодавство на предмет необхідності внесення відповідних змін;

– розробити типові архітектури ІКТ для державних органів;

– почати пілотне впровадження інформаційно-комунікаційної архітектури;

– створити «мобільний уряд»;

– розвинути проєкт «електронного уряду» й електронного врядування;

– розпочати впровадження нової моделі інформатизації переходу до хмарних технологій в органах державної влади та місцевого самоврядування.

У сфері економіки планується:

– почати поступове широке впровадження ІКТ в усі галузі;

– забезпечити масову підготовку і перепідготовку ІТ-фахівців;

– розробити підходи, потрібні для підвищення профільної комп’ютерної грамотності фахівців усіх галузей, і почати відповідне навчання.

В інформаційній сфері плануються:

– вдосконалення законодавства, що стосується ЗМІ;

– технічна модернізація вітчизняних ЗМІ;

– подальше розширення географії розповсюдження українських мас-медіа;

– підвищення кваліфікації співробітників, зайнятих у сфері реалізації державної інформаційної політики.

На другому етапі (2025−2030 роки) планується продовжити реалізацію заходів першого етапу, а також реалізувати заходи, спрямовані на впровадження і поширення результатів, отриманих на попередньому етапі.

5.3. Система інформаційного забезпечення державної безпеки України

Система інформаційного забезпечення державної безпеки України належить до загальної системи нацбезпеки і являє собою сукупність органів державної влади та підприємств, які узгоджено здійснюють діяльність із забезпечення інформаційної безпеки, керуючись спільними правовими нормами [159].

Організаційна структура цієї системи в Україні містить такі складові:

– органи державної влади та місцевого самоврядування, що виконують завдання забезпечення такої безпеки в межах власної компетенції;

– державні і міжвідомчі комісії та ради, спеціалізовані на питаннях інформаційної безпеки;

– структурні та міжгалузеві підрозділи із захисту інформації органів державної влади, відповідні структурні підрозділи підприємств, які проводять роботи з використанням відомостей, що вважаються державною таємницею, або спеціалізуються на захисті інформації;

– науково-дослідні, проєктні та конструкторські організації, які виконують роботи щодо забезпечення такої безпеки;

– навчальні заклади, які займаються підготовкою і перепідготовкою фахівців у розглядуваній сфері.

Важливу роль у системі інформаційної безпеки відіграють державні та громадські організації із спеціалізацією щодо контролю за діяльністю державних і недержавних ЗМІ.

Система інформаційного забезпечення держбезпеки України здійснює свою діяльність на основі відповідної політики. Склад цієї системи визначає Президент України.

До організаційної основи системи інформаційного забезпечення держбезпеки належать:

– Рада національної безпеки і оборони України [250];

– Кабінет Міністрів України [127];

– Міністерство аграрної політики та продовольства України [193];

– Міністерство внутрішніх справ України [194];

– Міністерство енергетики та захисту довкілля України [196];

– Міністерство розвитку економіки, торгівлі та сільського господарства України [204];

– Міністерство закордонних справ України [197];

– Міністерство культури і туризму України [199];

– Міністерство оборони України [201];

– Міністерство охорони здоров'я України [203];

– Міністерство освіти і науки України [202];

– Міністерство у справах сім'ї, молоді та спорту [200];

– Міністерство енергетики та вугільної промисловості України [195];

– Міністерство соціальної політики України;

– Міністерство промислової політики України;

– Міністерство інфраструктури України [198];

– Міністерство України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи;

– Міністерство фінансів України [206];

– Міністерство юстиції України [207];

– органи місцевого самоврядування;

– органи судової влади, які відповідно до законодавства України беруть участь у вирішенні завдань у розглядуваній сфері.

Учасниками цієї системи вважаються:

– власники об’єктів критичної інформаційної інфраструктури та організації, що експлуатують такі об’єкти;

– засоби масової інформації і масових комунікацій;

– організації грошово-кредитної, валютної, банківської та інших сфер фінансового ринку;

– оператори зв’язку;

– оператори інформаційних систем;

– організації, які займаються створенням та експлуатацією інформаційних систем і мереж зв’язку, а також розроблення, виробництвом та експлуатацією засобів забезпечення інформаційної безпеки та/або наданням послуг у цій сфері;

– організації, що здійснюють освітню діяльність у розглядуваній сфері;

– ГО;

– інші організації та громадяни, які відповідно до законодавства України є причетними до вирішення завдань із забезпечення інформаційної безпеки.

До завдань державних органів у межах їх діяльності з розвитку і вдосконалення системи інформаційного забезпечення держбезпеки належать такі:

– зміцнення управлінської вертикалі і централізація сил забезпечення інформаційної безпеки на всіх рівнях від загальнодержавного до муніципального й рівня конкретних окремих об’єктів інформатизації, операторів інформаційних систем і мереж зв’язку;

– удосконалення форм і методів взаємодії сил забезпечення такої безпеки для забезпечення їх кращої готовності протидіяти інформаційним загрозам, серед іншого завдяки регулярним навчанням (тренуванням);

– удосконалення інформаційно-аналітичних і науково-технічних аспектів функціонування розглядуваної системи;

– покращення взаємодії державних органів, органів місцевого самоврядування, різних організацій і громадян під час вирішення завдань у цій сфері.

У контексті функціонування системи інформаційного забезпечення держбезпеки в Україні Кабінету Міністрів України видав Розпорядження від 30.01.2019 «Про затвердження Плану заходів щодо реалізації концепції розвитку системи електронних послуг в Україні на 2019–2020 роки». Зокрема, протягом 2019 р. планувалося запровадити щонайменше 50 електронних послуг, які стосуватимуться:

– виробництва медикаментів;

– забезпечення водовідведення;

– надання послуг будівництва;

– оформлення водійських посвідчень тощо.

Важливою також є обставина, що в Україні поступово змінюється сама філософія розвитку таких послуг. Зокрема, у перспективі Державне агентство з питань електронного урядування України не лише розроблятиме нові сервіси електронного характеру, а й оптимізуватиме їх з урахуванням актуальних життєвих та бізнесових ситуації, зокрема шляхом об’єднання декількох окремих адміністративних послуг.

Відповідно, цільовими індикаторами подальшого впровадження електронних послуг в нашій державі є такі:

– збільшення рейтингу «електронного уряду»;

– підвищення індексу задоволеності населення якістю надання державних послуг;

– зниження індексу бюрократизації надання таких послуг;

– збільшення частки наданих електронних державних послуг по відношенню до загальної кількості послуг, отриманих у традиційному вигляді;

– розширення переліку мобільних версій цих послуг у загальному обсязі електронних послуг;

– розвиток автоматизованих функцій державних органів;

– збільшення частки оновленого (актуалізованого) картографічного матеріалу на територіях країни.

Передбачається, що сучасна телекомунікаційна мережа доступу і «електронний уряд» України слугуватимуть інфраструктурою створення інформаційного суспільства [65]. Зокрема, серед значущих нових напрямів розвитку «електронного уряду» буде вирішено такі завдання:

– перегляд життєвого циклу проєктів інформаційно-комп'ютерних технологій у бік впровадження модульного підходу, орієнтованого на короткі кроки і швидке досягнення конкретних результатів;

– ужиття заходів з усунення «вхідних порогів» для участі в державних інформаційно-комп'ютерних проєктах невеликих ІТ-компаній;

– формування Єдиного інформаційно-аналітичного середовища державних органів, що виступатиме головним інструментом узгодженого проведення всіх видів реформ держуправління;

– проведення ревізії і паспортизації всієї соціально значущої інфраструктури держави (інженерні мережі, житловий фонд, дороги тощо), створення нових державних баз даних;

– забезпечення єдиного національного геоінформаційного середовища, яке надасть державним органам доступ до сучасного, якісного та повного геоінформаційного матеріалу, інтегрованого з об'єктами обліку державних баз даних;

– системне вирішення на державному рівні завдання щодо збору і переведення в електронний вигляд історичних відомостей для державних баз даних, архівів та відомчих інформаційних систем;

– визначення переліку типових інформаційних систем та їх використання в державних і місцевих виконавчих органах в межах нової моделі інформатизації у вигляді «хмарних сервісів» на підставі аналізу процесів діяльності органів державної влади та місцевого самоврядування;

– подальше скорочення і спрощення бізнес-процесів із надання державних послуг та їх автоматизація;

– автоматизація функцій місцевих органів виконавчої влади;

– розроблення єдиної системи нумерації та кодування адміністративних документів;

– інтенсивний розвиток «мобільного уряду» − одного з напрямів «електронного уряду», призначеного для оперативного представлення результатів державних послуг для громадян і бізнесу за допомогою мобільних пристроїв;

– продовження роботи по значному скороченню обігу документів між державними органами шляхом удосконалення регламентів роботи з електронними документами, засвідчених електронним цифровим підписом, та впровадження Єдиної системи електронного документообігу на основі «хмарних сервісів» і роботи на мобільних пристроях із криптографічним захистом інформації;

– ужиття заходів щодо інтеграції комерційних і державних систем і сервісів;

– регламентація питань використання ліцензійного та вільного програмного забезпечення;

– заснування єдиного Call-центру з надання державних послуг, серед іншого прийняття скарг на якість надання цих послуг та оповіщення про статуси і їх готовність;

– формування Єдиного особистого кабінету громадянина, призначеного для офіційної інформаційної взаємодії юридичних та фізичних осіб з державними органами й організаціями щодо надання державних і недержавних послуг і використання персональних даних;

– проведення робіт по розвитку інфраструктури запису електронно-цифрового підпису;

– суттєве збільшення кількості пунктів громадського доступу до електронних послуг та оновлення обладнання вже діючих [65].

Зауважимо, що в Україні варто також розробити державну цільову програму «Електронна Україна−2030», покликану налагодити діалог між державними структурами та громадянським суспільством. На базі розвитку сучасних методів інформаційного обміну між ними з’являться принципово нові можливості для забезпечення інформаційної відкритості та гласності ухвалення рішень, а також взаємодії між суспільством та органами державної влади, і як наслідок підвищення рівня довіри до останньої. Ця програма має бути розрахована на 10 років.

Водночас провадження інформаційної політики забезпечення держбезпеки й використання новітніх інформаційних технологій потребують значних інвестицій. На жаль, в нашій країні традиційно приділялося недостатньо уваги розвитку інформаційних технологій і комунікацій. Тому необхідно стимулювати українські бізнес-спільноти вкладати гроші в інформаційно-комунікативну систему і всіляко допомагати просувати український інформаційний продукт.

Конкуренція на українському ринку продовжує загострюватися, експансія найпотужніших інформаційних концернів – посилюватися до того ж із розширенням масштабів. Через це складається така ситуація, в якій кілька потужних інформаційно-видавничих об’єднань, залежних від фінансово-промислових груп, мають можливість монополізувати інформаційне обслуговування суспільства і держави; при цьому вони

переслідують не громадські, а своєкорисливі інтереси згаданих груп. Єдиною можливістю запобігти розвитку такої ситуації, що може призвести до остаточної втрати незалежності ЗМІ й обмеження свободи журналістської діяльності є розроблення й ухвалення правової бази для боротьби з монополією у цій галузі [217].

Наявний механізм реалізації політики інформаційного забезпечення державної безпеки зараз не є досконалим і не дасть бажаних результатів, бо очевидно, що в ситуації, де існує лише обмежена кількість джерел , а ринок надання інформації захопили й поділили олігархічні або близькі до олігархів структури він не може працювати ефективно. Оскільки олігархів менше за все цікавить громадянське суспільство, так само як і інтереси та потреби населення в об'єктивній інформації, а висвітлення діяльності державних структур здійснюється тільки під тиском окремих держслужбовців, то зрозуміло, що за такого стану справ внутрішня інформаційна політика держави в цілому і державних структур зокрема здійснюється фактично за допомогою тиску чиновників на олігархів або, навпаки, − тиску олігархів на чиновників.

Для того щоб система була ефективною, необхідно дотримуватися плюралізму думок і брати до уваги те, що механізм реалізації інформаційної політики може бути ефективним лише за наявності налагодженої комунікації між державою і громадянським суспільством, інакше конфлікт і пов'язані з ним наслідки є неминучими. Ігнорування евристичних можливостей діалогу, розуміння і комунікативних зв'язків призводить до конфлікту. У разі настання конфліктів і криз порушуються часові й історичні зв'язки, а також втрачається узгодженість змістовних зв'язків, що об'єднують історію в певну єдність, а суспільство − в якусь цілісність.

Ураховуючи те, що суспільство поділене на різні політичні напрямки, держава повинна всіма силами сприяти налагодженню нормальних відносин між учасниками політичної боротьби і в жодному разі не ігнорувати

прохання та сподівання політичних сил, а навпаки, бути більш уважною до суспільних процесів, адже сучасна розвинена держава − це насамперед демократична правова держава, в якій дотримуються права і свободи людини та громадянина. Державні структури, особливо силові, часто наполягають на тому, що безпека важливіша за свободи, і треба контролювати потоки інформації для того, щоб припиняти діяльність різних радикалів. Але треба при цьому дотримуватися надзвичайної обережності, щоб не перетнути межу і не дозволити втратити взаємозв'язок між громадянським суспільством і державою, гарантувати свободу слова для добропорядних і законослухняних громадян, які мають право на таємницю листування і недоторканність приватного життя. Принциповою відмінною рисою демократичної форми управління є постійна взаємодія між державною владою і громадянським суспільством, що ґрунтується на взаємній повазі, довірі та рівноправному діловому партнерстві. Лише за наявності такої взаємодії можна реально забезпечити відповідність держуправління таким загальновизнаним у політології критеріям демократичної держави, як:

– підзвітність влади;

– відкритість;

– адекватна реакція на зміни зовнішнього середовища або сигнал зворотного зв'язку, тобто сприйнятливість.

Підзвітність державних структур громаді та суспільству може проявлятися у разі проведення цими структурами грамотної інформаційної політики та названої вище політики відкритості та сприйнятливості до прохань громадян. Державі треба визначитися, чи є завдання з інформаційного забезпечення діяльності уряду першочерговим. Це має значення під час розподілу, наприклад, фінансових ресурсів, оскільки пріоритетні напрями діяльності уряду або інших окремих державних органів і структур завжди потребують великих масштабів фінансування, щоб вирішувати поставлені суспільством завдання.

Механізм реалізації інформаційної політики буде ефективним лише у разі серйозного підходу з боку державних структур до виконання цього завдання. Якщо ж інформаційна політика провадиться виключно з метою позитивно характеризувати дії уряду, то це зовсім інша справа. Не можна недооцінювати спроможності сучасних інформаційних технологій і розглядати інформаційну політику як щось додаткове, не основне, і взагалі ставитися до неї як до другорядного завдання, адже, по суті, державна інформаційна політика дедалі сильніше виступає системоутворюючим елементом сукупної діяльності всієї держави, а також найважливішим засобом підтримання публічного діалогу влади й суспільства. Завдяки такій позиції вона здатна не лише досягати власних цілей, але і компенсувати невдачі держуправління в решті сфер діяльності та суспільного життя. Втім, із тих само причин ця політика у разі слабкого опрацювання державних планів в інформаційній сфері може і погіршити невдачі уряду.

Викликають деякий сумнів лише два положення. Перше стосується твердження, за яким успішно реалізована державна інформаційна політика дійсно може компенсувати невдачі держуправління в інших сферах. Якщо уряд хоче залишатися при владі до кінця встановленого терміну і, можливо, навіть продовжити свої повноваження, то він не повинен займатися маніпуляціями з інформацією і вводити населення в оману, оскільки це може серйозно нашкодити як уявленням про сам уряд, так і іміджу політичних партій. Інше сумнівне положення – твердження, що буцім така політика виступає системоутворюючим елементом сукупної діяльності всієї держави. Зрозуміло, що інформаційна політика пронизує всі сфери життєдіяльності держави, але залишається, тим не менш, не стільки системоутворюючим елементом її діяльності, скільки засобом підтримання її діалогу з громадянським суспільством. Насправді системоутворюючим елементом виступає соціальна сфера життєдіяльності держави і, отже, соціальна політика. Головне − це люди, тому на першому місці у будь-якій

цивілізованій державі повинно стояти вирішення соціальних завдань, а вже потім – усе інше, включно з розробленням і провадженням інформаційної політики. Неефективне управління країною в поєднанні з дієвою внутрішньою інформаційною політикою не принесе бажаних результатів і ніяк не буде сприяти поліпшенню якості життя. Тому думка, що буцім грамотна інформаційна політика здатна компенсувати невдачі уряду в решті сфер держуправління, є хибною. Натомість упровадження новітніх технологій сприяє поліпшенню роботи уряду, і з цим твердженням сперечатися важко, оскільки новітніми технологіями користуються всі розвинені демократичні країни світу.

Якщо Україна хоче стати відкритою для власних громадян державою і незалежною від іноземних технологій в інформаційній сфері, то треба розвивати аналогічні вітчизняні технології і, відповідно, робити значні капіталовкладення в цю сферу. Через це дуже важливе значення має створення умов для пріоритетного розвитку вітчизняних нових інформаційних і телекомунікаційних технологій, виробництва технічних і програмних засобів, що сприятимуть досягненню сучасного рівня розвитку телекомунікаційних мереж і високоінтелектуальних інформаційних послуг в усьому інформаційному просторі (включно з міжнародним) [268].

Розвивати власні згадані технології необхідно у будь-якому разі, і чим швидше, тим краще, оскільки відставання України за показником їх розвитку від більшості розвинених країн вже є істотним продовжує збільшуватися. Так, на цей момент Україна відстає у сфері інформаційних технологій, виробництві сучасних великих інтегральних схем і надмініатюрних комплектуючих виробів, оцифровуванні електронного обладнання й розвитку цифрових телекомунікаційних мереж технічних засобів. До того ж, щоб забезпечити інформаційну безпеку нашої держави, технології мають бути вітчизняними. Вкладати інвестиції в розвиток зазначених вітчизняних технологій можуть як держава, так і приватні компанії відповідної

спеціалізації, зацікавлені у виробництві того чи іншого інформаційного продукту. При цьому необхідно не лише залучати інвестиції, а і стежити за їх цільовим використанням. Саме держава має контролювати використання коштів, що виділяються на розроблення інформаційних і телекомунікаційних проєктів. Лише спільними зусиллями держави і приватного бізнесу можна зробити ривок в інформаційній сфері і наздогнати іноземних конкурентів і «за сумісництвом» − постійних опонентів на міжнародній арені.

Великі капіталовкладення необхідні для розвитку інформаційної сфери, і це не благодійність, а прибутковий бізнес, що працює на самоокупності без будь-яких дотацій від держави. За оцінками фахівців, один долар, вкладений в інформаційну галузь, дає в 10 разів більше прибутку, ніж нафтова промисловість. Отже, держава, намагаючись реалізувати свої цілі, але, не маючи при цьому права ризикувати грошима платників податків, має вибирати відповідні способи реалізації таких цілей. Крім того, вона повинна акціонувати свої інформаційні структури, що приносять стійкий прибуток, щоб використовувати їх діяльність для потреб населення. Пересічні громадяни, швидше за все, довірятимуть тому телевізійному каналу, акціонерами якого вони є, і механізм реалізації інформаційної політики буде більш ефективним [97].

Найкращою запорукою успішної реалізації інформаційної політики є довіра з боку населення і можливість для громадян стати акціонерами державної телерадіомовної компанії, що обов’язково породить у них ентузіазм.

Громадське телебачення можна назвати громадським інститутом громадянського суспільства. Його завдання – забезпечувати громадян незаангажованою інформацією. Створення такого інституту піде лише на користь механізму реалізації внутрішньої інформаційної політики. Після створення громадського (незалежного) телебачення механізм реалізації внутрішньої інформаційної політики демократичної держави стане більш

досконалим, оскільки зросте довіра суспільства до ЗМІ. На думку фахівців, держава вважається стабільною, якщо засобам масової інформації довіряють не менше 40 % громадян, якщо ж планка опускається нижче 40 %, то це має стати тривожним сигналом державі і самим цим засобам. Зниження довіри громадян до масової інформації зазвичай відбувається в результаті постійних маніпуляцій держави і ЗМІ стосовно певних питань і може сприяти наростанню революційних настроїв населення, особливо в перехідних суспільствах [363]. Державі треба дбати про стабільність у суспільстві і заради її збереження не займатися різними авантюрами в інформаційній сфері. Водночас їй слід розуміти, що наразі інформація є вихідним ресурсом для формування державної політики та здійснення державного управління в усіх сферах життя і діяльності суспільства та держави. Інформаційне забезпечення діяльності органів державної влади та своєчасне забезпечення їх системи достовірною інформацією є найважливішою умовою:

– сталої та ефективної роботи державного механізму;

– реалізації всіх стадій процесу держуправління;

– адекватного цілям і завданням розвитку і задоволення насущних потреб суспільства.

Держава сама зацікавлена мати достовірну інформацію, і це сприятиме поліпшенню роботи органів державної влади. Але слід зауважити, що, наприклад, у воєнний час необхідно обмежувати інформацію, і якщо є достовірна інформація від якоїсь терористичної організації у вигляді листа або відеозапис із зверненням лідера терористів, то цю інформацію необхідно передавати лише закритими каналами зв’язку і не передавати в ефір. Своєчасне забезпечення окремих (силових) державних структур достовірною інформацією про заплановані злочини може врятувати багато життів, але поява інформації про підготовку терактів в ефірі телеканалів нікому на користь не піде. Нічого, крім паніки серед населення, така інформація

викликати не може, і про це треба пам’ятати керівникам ЗМІ та всім особам, відповідальним за їх інформаційну політику.

Важливою особливістю інформаційного забезпечення діяльності системи органів державної влади є те, що державна влада повинна забезпечувати, з одного боку, громадянські свободи, захист персональних даних і збереження особистої таємниці, а з іншого − захищати національну інформаційну безпеку, охороняти правопорядок і досягати дотримання законів. Для багатьох нових інформаційних технологій, що стосуються збирання, аналітичної обробки і поширення персоніфікованих даних, потрібні особливі заходи захисту інформації. Тому, беручи на озброєння будь-які нові інформаційні технології, держава повинна водночас із цим застосовувати і нові відповідні технології, що забезпечуватимуть їх безпеку. У свою чергу, інформаційну безпеку покликано забезпечити захист життєво важливих інтересів особи, суспільства і держави від зовнішніх і внутрішніх загроз, до яких, серед іншого належать антидержавна й антигромадська діяльність деяких іноземних держав і внутрішніх громадських та бізнесових структур стосовно формування, поширення і використання інформації. Одним із головних обов’язків держави є турбота про те, як забезпечити своїм громадянам безпеку, серед іншого інформаційну, та як на законодавчому рівні обмежити можливість поширювати інформацію, що пропагує екстремізм і насильство, закликає до міжнаціональної ворожнечі тощо [99].

Практика показує, що крім спеціальних рекомендацій для ЗМІ, що стосуються заборон на пропаганду насильства і демонстрацію виступів екстремістів, треба ввести обмеження і на правовому рівні, оскільки самі ЗМІ обмежувати себе не хочуть. Необхідно, щоб їхні представники самі усвідомили те, що свобода слова передбачає і відповідальність за сказані слова.

Так, коли йдеться про масову інформацію, яку споживає суспільство, ЗМІ мають усвідомлювати, що вони роблять свій внесок у формуванні

громадської думки, і відчувати свою відповідальність за це. Масова інформація − це соціальна інформація, якою оперує маса, оскільки така інформація народжується у масовій аудиторії, оскільки вона поширюється по масовим каналам, або тому, що ця інформація споживається масовою аудиторією [347].

Так чи інакше, відповідальною за суспільство і громадську безпеку є держава, і саме їй треба подбати про те, щоб ЗМІ були соціально відповідальними. Що стосується бажання еліти (адже власники медіа-холдингів є частиною еліти), то їх побажання та пропозиції треба враховувати, але не сприймати як абсолютну істину та заклик до дії. Законодавча гілка влади повинна активно займатися питаннями правового обмеження певних антигромадських та аморальних дій з боку ЗМІ.

Громадянське суспільство шляхом створення ГО має можливість чинити вплив на ухвалення рішень, серед іншого і на інформаційну політику ЗМІ, які зобов'язані діяти в межах закону. Звісно, треба враховувати те, що ці засоби здатні іноді просто ігнорувати потреби суспільства і керуватись у своїх діях ліберальною теорією, за якою ЗМІ суспільству нічого не винні. У громадянського суспільства є спосіб впливу і в таких випадках. Наприклад, якщо відразу десять впливових громадських організацій закличуть громадян не купувати продукцію того чи іншого видання, − це змусить журналістів піти на уступки і внести зміни в свою інформаційну політику. Так само У громадянське суспільство може впливати і на державні ЗМІ – знову ж таки за допомогою ГО, що надсилають свої пропозиції і побажання в письмовому вигляді в державні структури. Держава, зацікавлена в стабільності, уважно вивчатиме всі пропозиції та побажання таких організацій, які уособлюють громадянське суспільство [18].

Формування державної інформаційної політики зазвичай спирається на такий фундаментальний принцип (чи то закономірність): вказана політика повинна задовольняти і захищати інтереси держави тією мірою, якою сама

держава реалізує і захищає інтереси громадянського суспільства та кожної особи. Якщо ж держава не захищає інтереси громадянського суспільства, то цю роль можуть відігравати ЗМІ. Коли ж і вони цього не роблять, тоді в народу та громадянського суспільства починається криза довіри і до держави, і до ЗМІ.

Іншими впливовими компонентами політичної організації суспільства є партії, які можуть впливати на державу за рахунок наявності своїх представників у законодавчій і виконавчій гілках влади.

Ясна річ, сучасні політичні системи важко уявити без політичних партій, бо саме вони забезпечують плюралізм думок у парламенті та захищають інтереси своїх виборців. Їх взаємовідносини із ЗМІ завжди були дуже тісними, оскільки преса історично проникала в суспільство як орган партійної інформації, і саме за допомогою газет партії реалізовували свою інформаційну політику. Багато партій і зараз популяризують свої ідеї та погляди за допомогою друкованої продукції і займаються випуском газет, які є органами партійної пропаганди [9].

Фактично система, за якої ЗМІ виступають «рупорами» різних політичних партій, може цілком ефективно функціонувати і розвиватися, тому що партії являють собою різні політичні сили в суспільстві і, відповідно, забезпечують плюралізм думок. Такий механізм реалізації внутрішньої інформаційної політики буде ефективний, якщо жодна з партій не буде мати переваги перед іншими, і всі вони матимуть рівний доступ до ЗМІ. Однак на практиці це складно здійснити, оскільки великі партії мають більше ресурсів і, відповідно, більше можливостей для реалізації своєї інформаційної політики, і така система дуже скоро перетвориться на олігополію, що зводиться до кількох великих учасників. Цього можна уникнути за наявності незалежного телебачення і чесних журналістів, які зможуть забезпечити населення незаангажованою інформацією, що теж досить складно.

Партії створюються, щоб прийти до влади, інакше кажучи, досягнення вищої політичної влади є головною метою, сенсом існування будь-якої партії. Безпосередньою метою їх створення і діяльності є політична мета, тобто мета, якимось чином пов'язана з владою. Зазвичай її змістом є формування та реалізація внутрішньої і зовнішньої політики держави, політичний та ідеологічний вплив на різні верстви, прошарки, класи і структури суспільства на певному етапі його розвитку.

Для того щоб впливати на населення і популяризувати свої погляди, партіям необхідно мати доступ до ЗМІ, особливо в період виборчих кампаній, коли між партіями точиться запекла боротьба за голоси виборців. У разі перемоги на виборах до парламенту партія одразу ж збільшує свої інформаційні можливості, оскільки депутати цієї партії виступатимуть з трибуни парламенту, що, в свою чергу, широко висвітлюється в пресі. Природно, що головною метою партій, які перемогли на виборах у парламент, є не позування перед журналістами, а законотворча діяльність на благо суспільства.

Також у результаті провадження державної цільової програми «Електронна Україна–2030» очікується покращення діалогу між державою, населенням і бізнесом.

Зауважимо, що наразі:

– створено механізми діалогу та зворотного зв'язку держави з населенням і бізнесом; зокрема, всі державні органи мають тепер власні інтернет-ресурси з інформацією для громадян і бізнесу;

– законодавчо закріплено вимоги щодо забезпечення доступу до інтернет-ресурсів державних органів для інвалідів;

– проводиться оцінювання повноти й якості інформації на Інтернет-ресурсах державних органів;

– на більшості порталів державних органів реалізовано послугу «Віртуальна приймальня», де громадяни безпосередньо звертаються в державні органи;

– ведуться блоги перших керівників державних органів та Уряду Республіки України, де кожен бажаючий може залишати коментарі і ставити запитання;

– регулярно проводяться інтернет-конференції за участю членів Уряду та представників органів влади, під час яких громадяни отримують відповіді на свої питання в інтерактивному режимі.

Зазначені заходи покликано підвищити прозорість і підзвітність діяльності державних органів для реалізації прав і задоволення законних інтересів громадян і суспільства в цілому щодо інформації.

У цьому контексті передбачається досягти такі цільові індикатори:

– підвищення індексу е-участі нашої держави;

– зростання кількості активних додатків, які базуються на сервісах порталів «відкритих даних» та активно використовуються.

Відповідно, для систематизації збору даних та структурування інформації державних органів доцільно реалізувати такі заходи:

– розширити перелік публічної інформації, що надається Урядом України і державними органами громадянам і бізнесу ;

– внести зміни у чинне законодавство з метою забезпечення своєчасності надання, об’єктивності, повноти та достовірності інформації на відповідних електронних ресурсах, яка за законодавством України має обов’язково публічно розповсюджуватися або надаватися державними органами;

– створити й удосконалювати портал «електронного уряду», який, зокрема, служитиме майданчиком для діалогу з населенням, обговорення якості надаваних державних послуг, зокрема консолідації даних щодо

планування і фактичного освоєння бюджетних коштів державними органами [129];

– активно залучати громадян, неурядові та інші недержавні організації у процес постійного громадського моніторингу якості надання державних послуг;

– користуватись соціальними майданчиками в Інтернеті для широкого обговорення соціальних проблем державними органами і населенням;

– створити та почати використовувати механізм залучення громадян у процес реформування та поліпшення держави;

– уніфікувати сайти державних установ та перевести їх на єдину платформу;

– реалізувати механізми електронного оцінювання громадянами ефективності роботи органів державної влади та місцевого самоврядування.

Висновки до п’ятого розділу

1. Зазначено, що Концепція інформаційного забезпечення державної безпеки покликана забезпечити єдність підходів до розроблення та втілення у життя відповідної державної політики, а також методологічне підґрунтя для вдосконалення заокнодавства, що стосується цієї сфери. Відповідно, метою згаданої Концепції є розбудова державної системи забезпечення інформаційної безпеки, яка гарантуватиме захист національних інтересів України в інформаційній сфері.

Обґрунтовано, що реалізація Концепції інформаційного забезпечення державної безпеки допоможе:

– реалізувати громадянам передбачені Основним законом права на отримання, зберігання і поширення повної, достовірної та своєчасної інформації;

– забезпечити рівноправну участь України у світових інформаційних відносинах;

– ефективному інформаційному забезпеченню політики держави;

– забезпечити надійність і стійкість функціонування критично важливих інформаційних систем;

– налагодити безперебійне функціонування і надійний захист єдиного національного інфопростору.

Показано, що реалізація завдань зазначеної Концепції інформаційного забезпечення державної безпеки вимагає розвитку трьох напрямів:

1) законодавчого та нормативно-методичного;

2) організаційно-розпорядчого й організаційно-технічного;

3) кадрового.

2. Показано, що у напрямі організаційно-розпорядчого й організаційно-технічного забезпечення інформаційного забезпечення держбезпеки необхідно реалізувати комплекс заходів щодо забезпечення інформаційної безпеки критично важливих об’єктів інформатизації та розробити й запровадити єдину державну політику в розглядуваній сфері, серед іншого щодо системи захисту інформації. Для вирішення цього питання треба створити єдину державну систему моніторингу інформаційного простору й Оперативний центр забезпечення інформаційної безпеки разом з його інформаційною системою та інфраструктурою.

Підкреслено, що згадана вище єдина державна політика має за мету забезпечити розроблення та реалізацію єдиних стандартів у сфері забезпечення вимог до інформаційної безпеки як державних, так і недержавних інформаційних систем, ресурсів і підтримуючої інфраструктури.

3. Обґрунтовано, що ефективність роботи державних органів доцільно підвищувати за допомогою застосування архітектурного підходу, який передбачає автоматизацію діяльності державних органів шляхом створення узгодженої з уповноваженим органом інформаційно-комунікаційної архітектури для кожного такого органу.

Інформаційно-комунікаційна архітектура державного органу є сукупністю документів, моделей, матриць і діаграм, у яких міститься детальний опис поточного й планованого стану цього органу, а також план заходів з оптимізації взаємозалежностей і взаємозв'язків між функціями, бізнес-процесами, даними, інформаційними системами і компонентами технічної інфраструктури у межах плану інформатизації для забезпечення втілення в життя стратегічних цілей і завдань цього органу. Інформаційно-комунікаційна архітектура створюватиметься на основі моделі, яка складається з таких пов'язаних між собою компонентів:

– архітектура діяльності;

– архітектура даних;

– архітектура додатків;

– технологічна архітектура;

– архітектура інформаційної безпеки.

Зауважено, що, крім цього, слід розробити інформаційно-комунікаційну архітектуру органів місцевого самоврядування, яка дозволить уніфікувати діяльність державних органів у регіонах за рахунок використання єдиних бізнес-процесів, шаблонів документів, стандартів і типових рішень у межах ІКТ.

4. Доведено, що необхідно сформувати національну стратегію інформаційного забезпечення державної безпеки, що передбачатиме консолідації всіх прошарків суспільства для досягнення цілей інформаційного й інноваційного розвитку, а також координації діяльності бізнесу, всіх громадських інститутів та громадян з реалізації цієї Стратегії.

На підставі врахування міжнародного досвіду зазначено, що у формуванні інформаційного суспільства в контексті Стратегії інформаційного забезпечення державної безпеки треба визначити чотири ключові напрями:

1) забезпечення ефективності системи держуправління;

2) забезпечення доступності інформаційно-комунікаційної інфраструктури;

3) створення інформаційного середовища для соціально-економічного і культурного розвитку суспільства;

4) розвиток вітчизняного інфопростору.

Відзначено, що в згаданій вище Стратегії необхідно передбачити умови для забезпечення громадянам можливостей освоїти інформаційні технології та отримати навички роботи з ними за допомогою електронної освіти, довічного навчання і підготовки, дистанційної роботи, а також отримання послуг доступної електронної охорони здоров'я. Крім того, щоб зробити вітчизняну економіку більш відкритою, доступною та конкурентоспроможною, у цій Стратегії слід передбачити максимальне впровадження інтелектуальних систем в основні галузі економіки.

5. Підкреслено, що для систематизації збору даних та структурування інформації державним органам варто вжити таких заходів:

– розширити перелік публічної інформації, що надається Урядом України і державними органами громадянам і бізнесу ;

– внести зміни у чинне законодавство з метою забезпечення своєчасності надання, об'єктивності, повноти та достовірності інформації на відповідних електронних ресурсах, яка за законодавством України має обов'язково публічно розповсюджуватися або надаватися державними органами;

– створити й удосконалювати портал «електронного уряду», який, зокрема, служитиме майданчиком для діалогу з населенням, обговорення

якості надаваних державних послуг, зокрема консолідації даних щодо планування і фактичного освоєння бюджетних коштів державними органами [129];

– активно залучати громадян, неурядові та інші недержавні організації у процес постійного громадського моніторингу якості надання державних послуг;

– користуватись соціальними майданчиками в Інтернеті для широкого обговорення соціальних проблем державними органами і населенням;

– створити та почати використовувати механізм залучення громадян у процес реформування та поліпшення держави;

– уніфікувати сайти державних установ та перевести їх на єдину платформу;

– реалізувати механізми електронного оцінювання громадянами ефективності роботи органів державної влади та місцевого самоврядування.

6. Обґрунтовано, що система інформаційного забезпечення держбезпеки будується, враховуючи розмежування повноважень органів законодавчої, виконавчої та судової влади у цій сфері та предмети відання органів державної влади та місцевого самоврядування, що визначаються законодавством України у безпековій сфері.

Доведено, що зазначена система має забезпечувати гнучке управління процесами інформаційної безпеки на державному, регіональному, галузевому, виробничому і користувальницькому рівнях.

7. Відзначено, що в Україні доцільно розробити розраховану на 10 років державну цільову програму «Електронна Україна−2030», покликану налагодити діалог між державними структурами та громадянським суспільством. На базі розвитку сучасних методів інформаційного обміну між ними з’являться принципово нові можливості для забезпечення інформаційної відкритості та гласності ухвалення рішень, а також взаємодії

між суспільством та органами державної влади, і як наслідок підвищення рівня довіри до останньої.

Підкреслено, що поінформованість населення про діяльність держави забезпечуватиметься серед іншого шляхом прямої взаємодії державних органів з аудиторією ЗМІ, включно з технологією краудсорсингу.

Зазначено, що також доцільно розробити єдине інформаційно-аналітичне середовище державних органів, що слугуватиме головним інструментом узгодженого здійснення всіх видів реформ держуправління.

ВИСНОВКИ

У дисертації на доктринальному рівні вирішено важливу й актуальну для науки державного управління проблему, яка полягає в системному аналізі стану та перспектив національної безпеки держави в інформаційної сфері, розробленні нових підходів до вирішення проблемних питань і підготовці науково-прикладних рекомендацій щодо формування та реалізації державної інформаційної політики держави в контексті національної безпеки.

Абсолютно очевидно, що відсутність чіткої стратегії з реалізації державної інформаційної політики призводить не лише до погіршення загальної ситуації, але й серйозних загроз у сфері інформаційної безпеки держави. Саме тому все більшої актуальності набуває вироблення державної концепції інформаційної безпеки саме в сучасних умовах. У зв’язку з цим інформаційну безпеку можна розглядати як одну з обов’язкових умов функціонування сучасної держави.

Аналіз проблем у сфері інформаційної безпеки сучасних держав у цілому та України зокрема засвідчив, що їх державна політика спрямована на формування ефективної політики у сфері інформації і має розглядатися тільки в комплексі з урахуванням системного підходу, що працює в парадигмі функціонування теорії соціальних мереж. З огляду на це забезпечення ефективної системи державного управління національною безпекою України, де інформаційна безпека розглядається як її найважливіша ланка, можливо з урахуванням реалізації наступних основних висновків дисертації, які конкретизуються в таких положеннях:

1. Розкрито сутність інформаційної політики як феномена інформаційного суспільства та забезпечення його безпеки. Узагальнено сучасні теоретико-методологічні та державно-управлінські підходи у сфері розвитку інформаційної політики як невід'ємної частини функціонування інформаційного суспільства через виявлення критеріїв систематизації та

відповідних їм форм і видів інформаційного забезпечення національної безпеки, яка являє собою процес задоволення інформаційних потреб суб'єктів управління у сфері державної безпеки та виконує важливу багатопланову роль стосовно:

– визначення національних інтересів і пріоритетів національної безпеки;

– пошуку нових форм і способів забезпечення державної безпеки;

– впливу на діяльність суб'єктів управління безпекою, з урахуванням формування їх думки і поведінки відповідно до визначених пріоритетів і цінностей державної безпеки;

– розвитку всього механізму прийняття і реалізації державно-управлінських рішень у сфері державної безпеки.

Доведено, що інформаційному суспільству притаманні такі ознаки як:

– наявність єдиного інформаційного простору;

– домінування в економіці та управлінні нових технологічних укладів, що базуються на масовому використанні інформаційно-комунікаційних технологій;

– зростання ролі інфраструктури (телекомунікаційної, транспортної, організаційної) в системі суспільного виробництва і посилення тенденцій до спільного функціонування в економіці інформаційних і грошових потоків;

– зростання значущості проблем забезпечення інформаційної безпеки особистості, суспільства і держави, наявність ефективної системи забезпечення прав громадян і соціальних інститутів на вільне отримання, розповсюдження і використання інформації;

– високий рівень освіти, обумовлений розширенням інформаційного обміну на міжнародному, національному та регіональному рівнях, і відповідно підвищена роль кваліфікації, професіоналізму і здібностей до творчості як найважливіших характеристик праці;

– провідна роль інформаційних ресурсів у забезпеченні сталого

поступального розвитку суспільства;

– фактичне задоволення потреб суспільства в інформаційних продуктах і послугах.

2. Доведено, що методологічні основи інформаційного забезпечення державної політики безпеки держави забезпечуються якісною і високоефективною політикою органів державної влади, яка визначається наступними сутнісними характеристиками: по-перше, вибором форм, методів і способів її здійснення; по-друге, структурою національної безпеки і специфікою реалізації державної інформаційної політики в конкретних умовах. Крім того, показано, що зміст інформаційного забезпечення національної безпеки визначається також і характером інформаційних зв'язків суб'єктів національної безпеки, які пов'язані: з обміном інформацією між суб'єктами забезпечення національної безпеки, що забезпечують створення цілісної організаційної системи; інформаційними зв'язками між людьми, безпосередньо і опосередковано пов'язаними із забезпеченням функціонування системи національної безпеки; інформаційними зв'язками між технічними компонентами системи державної безпеки, оскільки частина інформаційних функцій надмірні для людини, проте є необхідними для забезпечення національної безпеки в сучасних умовах.

Крім того, інформаційні зв’язки можна поділити на дві групи. Першу групу складають змістовні інформаційні зв’язки, які характеризуються структурною (пов’язаною) інформацією. Це зв’язки між елементами видів безпеки; між внутрішніми елементами кожного виду безпеки; між кожним видом безпеки і зовнішнім середовищем (під зовнішнім середовищем тут розуміються національні інтереси інших країн) і т. ін.

Другу групу представляють функціональні інформаційні зв’язки, які характеризуються оперативною інформацією. До них можна віднести суб’єктно-об’єктні зв’язки (між суб’єктами, об’єктами, між суб’єктами і об’єктами, а також усередині них); зв’язки між суб’єктами, об’єктами та

джерелами загроз, а також із зовнішнім середовищем. Разом з тим усю сукупність інформаційних зв’язків відносно національної безпеки можна поділити на зовнішні та внутрішні інформаційні зв’язки.

3. Розкрито значення інформаційної безпеки в державно-управлінських відносинах через організацію та здійснення певних принципів інформаційного забезпечення національної безпеки. Показано, що ефективна інформаційна безпека в державно-управлінських відносинах можлива з урахуванням впровадження інформаційного забезпечення національної безпеки за умови дотримання певних принципів. Видається, що найбільш важливими з них є такі:

– повнота інформаційного забезпечення. Результати пошуку повинні містити інформацію в повному обсязі, в той же час звести до мінімуму «шум» і виключити дезінформацію. Основне – вибрати таку пошукову стратегію, щоб споживач отримав інформацію, що відповідає не лише заданій тематиці, а й його інформаційним потребам;

– актуальність інформаційного забезпечення, завдання якого полягає в поданні споживачеві пріоритетної інформації, що відповідає умовам і в установлені терміни;

– точність і надійність інформаційного забезпечення, які полягають у наданні споживачеві всієї необхідної інформації з урахуванням потрібних видів і мовного оформлення, хронологічної глибини тощо;

– інформація повинна подаватись у зручній для споживача формі (машинопис, мікрофільм, екран дисплея тощо);

– диференційованість інформаційного забезпечення з урахуванням функцій споживача, його статусу та оперативності розв’язуваних ним завдань;

– системність інформаційного забезпечення, що проявляється в систематичному задоволенні інформаційних потреб на всіх етапах забезпечення національної безпеки і комплексності видів інформаційного

забезпечення з урахуванням категорій споживачів, характеру їх інформаційних потреб, специфіки завдань, що вирішуються.

У сучасних умовах, внаслідок протиріч влади і суспільства комунікативна діяльність органів влади характеризується такими ознаками, як недостатня відкритість, фрагментарність, маніпулятивність технік. У зв'язку з цим, , недостатня соціальна відповідальність влади й особливості її комунікації детерміновані інструментальним підходом. Публічні служби використовуються як інструмент збереження владних інтересів, конструювання одностороннього бачення смислів державно-управлінських рішень. В цілому комунікативна модель формування та підтримки відносин з суспільством характеризується як одностороння, в результаті чого утворюється розрив між реальною політикою і інформаційним продуктом, що створює негативні наслідки для легітимності влади.

4. Проаналізовано процес інформатизації державно-управлінських відносин у формуванні державної безпеки в умовах глобального інформаційного суспільства. Доведено, що процеси інформатизації мають чіткий зв'язок з безпечним стійким розвитком суспільства і держави, що основа глобального інформаційного суспільства та державного управління – знання або інтелектуально-інформаційний ресурс. Оцінюючи результати перспектив забезпечення інформаційної безпеки в умовах становлення глобального інформаційного суспільства, можна зробити такі висновки.

Сучасний етап розвитку інформаційного суспільства характеризується нерівномірністю розвитку й розподілу інформаційно-комунікаційних технологій у різних регіонах світу. Це явище отримало офіційну назву «цифровий розрив» або «інформаційне нерівність». На сучасному етапі існують значні відмінності не тільки між розвиненими країнами та країнами, що розвиваються, а й між різними соціальними групами населення в кожній країні.

В рамках розвитку інформаційного суспільства формується також

глобальна система інформаційної безпеки. Для еволюційного, поступального переходу України на новий етап розвитку необхідно забезпечити умову, за якої її національні інтереси будуть природною, невід'ємною складовою частиною інтересів глобального інформаційного співтовариства. Отже, інформаційна безпека України буде одним із складових елементів системи глобальної інформаційної безпеки.

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.

5. Здійснено порівняльний аналіз вітчизняного та закордонного досвіду розробки й впровадження інформаційного забезпечення державної безпеки. Зазначено, що відповідно до Європейської конвенції про кіберзлочинність (інформаційну безпеку), забезпечення інформаційної безпеки передбачало недопущення чи усунення таких суспільно-небезпечних діянь проти конфіденційності даних: протиправний доступ; перехоплення; порушення цілісності; втручання в роботу; виробництво, обіг та використання спеціальних засобів для комп'ютерних злочинів з використанням комп'ютерів; підроблення; інформаційне шахрайство.

Показано, що в Україні поточне інформаційне забезпечення державної безпеки характеризується наявністю таких проблем:

– малоефективна система державного регулювання національного медіапростору;

– низький рівень присутності у глобальному медіапросторі, високий рівень інформаційної залежності від іноземних держав і структур;

– ринкова стихійність впровадження засобів комп'ютеризації та

телекомунікаційних мереж;

– відсутність довгострокової державної стратегії щодо розвитку інформаційної сфери;

– недосконаліть законодавства про інформацію;

– недостатній рівень державної підтримки виробництва та розповсюдження інформаційної продукції.

6. Охарактеризовано особливості функціонування організаційно-правового механізму інформаційного забезпечення державної безпеки. Обґрунтовано, що сьогодні слід визнати відсутність єдиного правового поля стосовно регулювання інформаційного забезпечення державної безпеки. Зокрема зазначено, що в різних нормативних актах перераховується велика кількість таємниць, проте за розголошення не всіх з них передбачена відповідальність. Крім того, наголошено, що сучасне законодавство, яке регулює питання забезпечення інформаційної безпеки України, не розглядає інформаційну безпеку у форматі захисту інформаційної свободи.

Здійснено поділ органів державної влади спеціальної компетенції, що регулюють інформаційну безпеку, залежно від певного виду інформаційних відносин, які підлягають інформаційному впливу, та виокремлено такі їх групи:

– органи, які регулюють сферу інформаційних відносин у загальному контексті та впроваджують державну інформаційну політику (Державний комітет телебачення і радіомовлення України);

– органи, що розробляють і впроваджують державну мовну політику та державну політику стосовно захисту суспільної моралі (Міністерство культури та інформаційної політики України);

– органи, які регулюють функціонування сфери отримання і зберігання інформації (Державний служба статистики України та Державна архівна служба);

– органи, що проводять аналіз і моніторинг визначених типів

інформації (Державна служба фінансового моніторингу України).

Наголошено, що такий підхід не дозволяє повноцінно здійснювати забезпечення інформаційної безпеки в державі, відтак необхідно чітко визначити частку і межі участі держави у забезпеченні інформаційної безпеки, в тому числі через законодавче встановлення заборон і обмежень в інформаційній сфері.

7. Визначено напрями модернізації єдиної державної політики у сфері інформаційної безпеки:

– збір, систематизація й узагальнення інформації щодо стану процесів інформаційної безпеки на об’єктах управління, оцінка стану інформаційної безпеки в регіоні, виявлення невирішених проблем у забезпеченні інформаційної безпеки, надання необхідної інформації щодо стану інформаційної безпеки органам державної влади та місцевого самоврядування;

– контроль стану інформаційної безпеки на об’єктах управління;

– визначення пріоритетних напрямків забезпечення інформаційної безпеки в державі та регіонах;

– розробка і контроль виконання цільових програм із забезпечення інформаційної безпеки;

– організація науково-технічних досліджень і розробок у сфері забезпечення інформаційної безпеки в державі та регіонах, виконання вимог нормативних документів щодо забезпечення інформаційної безпеки;

– розробка та затвердження регіональних нормативних і методичних документів із забезпечення інформаційної безпеки (концепції, положення, вимоги, норми, моделі, методики, рекомендації, інструкції та інші документи);

– надання методичної допомоги підприємствам, установам та організаціям в підготовці до ліцензування, а також у діяльності, пов’язаній з наданням послуг у сфері інформаційної безпеки, створенням засобів

інформаційної безпеки, а також впровадження засобів контролю їх ефективності;

– методичне керівництво підготовкою, професійною перепідготовкою та підвищенням кваліфікації фахівців у сфері інформаційної безпеки;

– координація діяльності органів місцевого самоврядування зі створення муніципальних систем інформаційної безпеки.

8. Запропоновано шляхи вдосконалення державної системи інформаційної безпеки. Показано, що цілі державної системи інформаційної безпеки досягаються шляхом створення та реалізації механізму забезпечення інформаційної безпеки, що включає:

– органи державної системи інформаційної безпеки, які забезпечують виконання всієї повноти завдань і функцій у сфері інформаційної безпеки та наділені відповідними повноваженнями;

– систему планових законодавчих, організаційно-розпорядчих, нормативних та інформаційних документів, що регламентують і забезпечують діяльність органів державної системи інформаційної безпеки;

– технології, системи і засоби, що знаходяться у віданні органів державної системи інформаційної безпеки.

9. Сформульовано концептуальні положення інформаційного забезпечення державної безпеки. Обґрунтовано, що реалізація Концепції інформаційного забезпечення державної безпеки в кінцевому підсумку сприятиме:

– реалізації конституційних прав громадян на отримання, зберігання і поширення повної, достовірної та своєчасної інформації;

– рівноправній участі України у світових інформаційних відносинах;

– ефективному інформаційному забезпеченню державної політики;

– забезпеченню надійності та стійкості функціонування критично важливих інформаційних систем;

– безперебійному функціонуванню й надійному захисту єдиного

національного інформаційного простору.

10. Окреслено стратегічні орієнтири інформаційного забезпечення державної безпеки України. Доведено необхідність формування національної Стратегії інформаційного забезпечення державної безпеки в контексті консолідації всіх верств суспільства для досягнення поставлених цілей інформаційного й інноваційного розвитку, а також координації бізнесу, всіх суспільних інститутів та громадян щодо реалізації цієї Стратегії.

Зроблено висновок, що у Стратегії інформаційного забезпечення державної безпеки необхідно передбачити умови для створення можливостей громадянам освоїти й отримати навички роботи з інформаційними технологіями за допомогою електронної освіти, довічного навчання і підготовки, дистанційної роботи, а також отримання послуг доступної електронної охорони здоров'я. Крім того, з метою побудови більш відкритої, доступної та конкурентоспроможної економіки нашої країни у Стратегії інформаційного забезпечення державної безпеки слід передбачити максимальне впровадження інтелектуальних систем в основні галузі економіки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Агамирзян И. Мировой опыт реализации концепции «электронного правительства» [Электронный ресурс] / И. Агамирзян. – Режим доступа : http: // www/microsoft.com/rus/govermtnt/analytics.

2. Алексеева И. Ю. Возникновение идеологии информационного общества / И. Ю. Алексеева // Информационное общество. – 1999. – № 1. – С. 30–35.

3. Алексенцев А. И. О составе защищаемой информации / А. И. Алексенцев // Безопасность информации. – 1999. – № 2. – С. 5–7.

4. Ананьїн В. Інформаційна безпека у контексті сучасних подій в Україні / В. Ананьїн, О. Пучков // Вісник Київського національного університету імені Тараса Шевченка. – 2007. – № 14–15. С. 28–29.

5. Андреєв С. О. Цивільний захист як напрям державної політики з питань національної безпеки: аналіз законодавчих новацій / С. О. Андреєв // Стратегічні пріоритети. – 2015. – № 4. – С. 24−28.

6. Андронова О. Электронное правительство в Европе и мире [Электронный ресурс] / О. Андронова, А. П. Николаев. – СПб., 2001. – Режим доступа : http: // www_ci.ru/inform22_01/ 06oo.htm.

7. Арістова І. Державна інформаційна політика: організаційно-правові аспекти [монографія] / І. Арістова. – Харків : Вид-во ХНУВС, 2000. – 365 с

8. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти : монографія / За загальною редакцією О. М. Бандурки. – Харків : Ун-т внутрішніх справ, 2010. – 368 с.

9. Аронсон Э. Эпоха пропаганды: механизмы убеждения, повседневное использование и злоупотребление / Э. Аронсон, Э. Пратканис. – Санкт-Петербург.: Прайм-Еврознак, 2003. – 384 с.

10. Бакуменко В. Д. Методологія державного управління проблеми встановлення та подальшого розвитку / В. Д. Бакуменко // Вісник УАДУ. – 2003. – № 2. – С. 11–27.

11. Бакуменко В. Д. Формування державно-управлінських рішень: Проблеми теорії, методології, практики : монографія / В. Д. Бакуменко. – Київ : Вид-во УАДУ, 2000. – 328 с.

12. Бакуменко В. Д. Теоретичні та організаційні засади державного управління : навч. посіб. / В. Д. Бакуменко, П. І. Надолішній. – Київ : Міленіум, 2003. – 256 с.

13. Бакут П. А. Информационные ресурсы – вопросы теории и практики / П. А. Бакут //Научно-техническая информация. – 2007. – №11. – С.16−23. – (Серия «Организация и методика информационной работы»).

14. Баринов А. Информационный суверинитет или инфомационная безопасность? / А. Баринов // Національна безпека і оборона. – 2001. – № 1. – С. 70–76.

15. Барыкин В. М. Силы специальных операций и способы борьбы с ними / В. М. Барыкин, С.Л. Велесов // Военная мысль. – 2001. – №2. – С. 12–15.

16. Баришполец В. А. Информационно-психологическая безопасность: основные положення / В. А. Баришполец // Информационные технологии. − 2013. − № 2. – Т. 5. − С. 62−104.

17. Барсегян А. А. Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP / А. А. Барсегян, М. С. Куприянов и др. – СПб. : БХВ-Петербург, 2009. – 512 с.

18. Баштанник В. В. Трансформація державного управління в контексті європейських інтеграційних процесів : монографія / В. В. Баштанник. – Дніпропетровськ : ДРІДУ НАДУ, 2010. – 390 с.

19. Бебік В. М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблік рілейшнз : монографія / В. М. Бебік. – Київ: МАУП, 2005. – 440 с.

20. Бек Д. Спиральная динамика. Управляя ценностями, лидерством и изменениями в XXI веке / Д.Бек, К.Кован. – М. : Открытый мир, 2010. – 424 с.

21. Белоногов Г. Г. Еще раз о гносеологическом статусе понятия «информация» / Г. Г. Белоногов, Р. С. Гиляревский // Научно-техническая информация. Серия 2. Информационные процессы и системы. – 2010. – № 2. – С. 1–6.

22. Бєлоусова Н. Б. Основні вимоги НАТО щодо забезпечення безпеки інформаційного простору / Н. Б. Бєлоусова, П. А. Афанасьєва // Актуальні проблеми міжнародних відносин. 2011. – Вип. 102. – Ч. І. − С. 196−202.

23. Бєляков К. І. «Інформаційна» аксіоматика у праві: проблеми формування / К. І. Бєляков // Науковий вісник Юрид. академії МВС України. − 2011. − № 3. − С. 263 – 268 с.

24. Бєляков К. І. Інформаційна діяльність: зміст та підходи до класифікації / К. І. Бєляков // Інформація і право. − 2012. − № 1. − С. 63−96.

25. Бєляков К. І. Проблеми законодавчого регулювання у сфері користування інформацією з обмеженим доступом в Україні / К. І. Бєляков, Ю. П. Мірошник // Стратегічна панорама. – 2004. – № 3. – С. 171−177.

26. Белл Д. Социальные рамки информационного общества / Д. Белл ; сокращ. пер. Ю. В. Никуличева // Новая технократическая волна на Западе / под ред. П. С. Гуревича. – М., 1988. – С. 330.

27. Белоножкин В. И. Информационные аспекты противодействия терроризму / В. И. Белоножкин, Г. А. Остапенко. – М. : Горячая линия ; Телеком, 2009. – 112 с.

28. Берг А. И. Кибернетика и прогресс науки и техники / А. И. Берг, Б. В. Бирюков // Современное естествознание. – М. : Мысль, 1969. – С. 350.

29. Берестова Т. Ф. Функции разных видов информации как основа формирования многоуровневой структуры информационного пространства / Т. Ф. Берестова // Научно-техническая информация. Серия 1. Организация и методика информационной работы. – 2009. – № 8. – С. 3–12.

30. Бжезинский З. Великая шахматная доска. Господство Америки и его геостратегические императивы / З.Бжезинский. – М. : Междунар. отношения, 1994. – 256 с.

31. Бжезинский Зб. Выбор. Глобальное господство или глобальное лидерство / Зб. Бжезинский. – М. : Международные отношения, 2004. – 288 с.

32. Бжезинский З. Между двумя веками: роль Америки в эру технотроники / З. Бжезинский ; пер. с англ И. М. Максимовой. – М. : Прогресс, 1972. – 308 с.

33. Бжезинский З. Стратегический взгляд. Америка и глобальный кризис / З. Бжезинский ; пер. с англ. М. Десятовой. – М. : Астрель, 2012. – 287 с.

34. Брекенридж Д. PR 2.0: новые медиа, новые аудитории, новые инструменты / Д.Брекенридж. – М. : Эксмо, 2009. – 245 с.

35. Бойко-Бойчук О. В. Механізми державного управління: узагальнена модель [Електронний ресурс] / О. В. Бойко-Бойчук. – Режим доступу : concept.at.ua/load/0-0-0-34-20

36. Брусницын Н. А. Информационная война и безопасность / Н. А. Брусницын. – М. : Вита-Пресс, 2001. – 279.

37. Блюменау Д. И. Информация и информационный сервис / Д. И. Блюменау. – Л. : Наука,1989. – С. 120.

38. Борсуковский Ю. Подходы и решения: информационная безопасность / Ю. Борсуковский // Мир денег. − 2001. − № 5. − С. 41−42.

39. Брайант Дж. Основы воздействия СМИ / Дж. Брайант, С. Томпсон. – М. : София, 2004. – 432 с.

40. Брандман Э. М. Глобализация и информационная безопасность общества : монография / Э. М. Брандман. – М. : Изд-во ГПИБ, 2007. – 173 с.

41. Браун П. Посібник з аналізу державної політики / П. Браун. – Київ : Основи, 2000. – 243 с.

42. Буланов А. Г. Национальные подходы к определению информационной войны / А. Г. Буланов // Гуманітарний вісник Запорізької державної інженерної академії. – 2002. – № 11. – С. 164–170.

43. Буравльов Є. Науково-технічна безпека України в контексті глобалізації / Є. Буравльов, В. Стогній // Вісник НАН України. – 2005. – № 3. – С. 32–40.

44. Бурков В. Н. Модели и механизмы управления безопасностью / В. Н. Бурков, Е. В. Грацианский, С. И. Дзюбко, А. В. Щепкин. – М. : СИНЕГ, 2001. – 160 с.

45. Бутузов В. М. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Науково-практичний коментар / В. М. Бутузов, С. Л. Остапець, В. П. Шеломенцев. – Київ : Друкарня МВС України, 2010. − 86 с.

46. Валевський О. Л. Держава і реформи в Україні: аналіз державної політики в умовах трансформації суспільства : монографія / О. Л. Валевський. – К.: вид-во НАДУ, 2007. – 217 с.

47. Васильова Н. Державний брендінг: зарубіжний досвід та перспективи для України. Державний брендінг: що це таке? [Електронний ресурс] / Н. Васильова // Українська PR-ліга : сайт. Режим доступу: http://www.pr-liga.org.ua/2/33/412.

48. Ведунг Е. Оцінювання державної політики та програм / Е. Ведунг. – Київ : ВСЕУВИТО, 2003. – 350 с.

49. Велігура А. В. Дослідження шляхів розробки комплексів інформаційної безпеки / А. В. Велігура, Л. М. Дегтярьова, О. М. Степанова // Вісник Східноукраїнського національного університету імені В. Даля. – 2009. − № 6(136). − Ч. 1 – С. 154–161.

50. Венгеров А. Б. Категория «информация» в понятийном аппарате юридичекской науки / А. Б. Венгеров // Советское государство и право. − 1977. − № 10. − С. 70−71.

51. Вершинин М. С. Политическая коммуникация в информационном обществе / М. С. Вершинин. – Санкт-Петербург: Изд-во В. А. Михайлова, 2001. – 253 с.

52. Вепринцев В. Б. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник / В.Б. Вепринцев,

А. В. Манойло, А. И. Петренко, Д. Б. Фролов. – 2-е изд., стереотип. – М. : Горячая линия – Телеком, 2011. – 495 с.

53. Винер Н. Кибернетика / Н. Винер ; пер. с англ. – М., 1968.

54. Винер Н. Кибернетика и общество / Н. Винер ; пер. с англ. – М. : Иностр. лит., 1958. – С. 31.

55. Власенко И. С. Информационная война: искажение реальности / И. С. Власенко, М. В. Кирьянов. – М. : Канцлер, 2011. – 196 с..

56. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики. Київ : НІСД, 2016. − 528 с.

57. Волковский Н. Л. История информационных войн : т. 1 (с древнейших времён по XIX век), т. 2 (XX век) / под ред. И. Петрова. – Санкт-Петербург.: Полигон, 2003. – 736 с.

58. Воронцова Л. В. История и современность информационного противоборства /Л. В. Воронцова, Д. В. Фролов. – М. : Горячая линия ; Телеком, 2006. – 192 с.

59. Воротін В. Є. Державне управління регіональним розвитком України : монографія / В. Є. Воротін, Я. А. Жаліл ; за заг. ред. В. Є. Воротіна. – Київ : Вид-во НІСД, 2010. – 288 с.

60. Выдрин Д. И. Политика: история, технология, экзистенция / Д. И. Выдрин. – Киев : Лыбидь, 2001. – 432 с.

61. Гаєвський Б. А. Політичне управління : навч. посіб. / Б. А. Гаєвський, В. А. Ребкало, М. В. Туленков. – Київ: УАДУ, 2001. – 160 с..

62. Галака О. Основні тенденції розвитку та ймовірні форми воєн та збройних конфліктів майбутнього / О. Галака, О. Ільяшов, Ю. Павлюк // Наука і оборона. – 2007. -№4. – С.10–15.

63. Галатенко В. А. Основы информационной безопасности / В. А. Галатенко. − М. : Интернет-университет информационных технологий, 2003. − 280 с.

64. Герасименко В. А. Основы защиты информации / В. А. Герасименко.– М. : Инкомбук, 1997. − 537 с.

65. Голобуцький В. Концепція електронного урядування і сучасні потреби України / О. Голобуцький // Політичний менеджмент. – 2005. – № 5. – С. 75–76.

66. Голобуцкий А. П. Электронное правительство / А. П. Голобуцкий, О. Б. Шевчук. – Киев, 2002. – 170 с.

67. Головань С. М. Нормативне забезпечення інформаційної безпеки / С. М. Головань, О. С. Петров, В. О. Хорошко, Д. В. Чирков та ін. – Київ : ДУІКТ, 2008. – 533 с.

68. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення / Ю. О. Горбань // Вісник НАДУ. – 2015, №1. – С. 136–141

69. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – Київ: Інтертехнологія, 2009. – 164 с.

70. Горбулін В. Системно концептуальні засади стратегії національної безпеки України / В. Горбулін, А. Качинський. – Київ : Євроатлантикінформ, 2007. – 592 с.

71. Горбулін В. П. Стратегічне планування : вирішення проблем національної безпеки : монографія / В. П. Горбулін, А. Б. Качинський. – Київ : НІСД, 2010. – 288 с.

72. Горбулин В. «Гибридная война» как ключевой инструмент российской геостратегии реванша [Електронний ресурс] / Зеркало недели: сайт. – 23.11.2015. – Режим доступу: http://gazeta.zn.ua/internal/gibridnaya-voyna– kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-_.html.

73. Грачев Г. В. Манипулирование личностью: организация, способы и технологи информационно-психологического воздействия / Г. В. Грачев, И. К. Мельник. – М. : Алгоритм, 2002. – 288 с.

74. Гриняев С. Н. Поле битвы – киберпространство: теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. – Минск : Харвест, 2004. – 448 с.

75. Гриняев С. Н. Информационная война: история, день сегодняшний и перспектива / С. Н. Гриняев // Агентура.ру : сайт Архивировано из первоисточника 4 июня 2012. – http://www.agentura.ru/.

76. Громадяни у пошуках інформації: українські реалії / упоряд. С. Г. Підлуська.– Київ : Україна, 2005. – 180 с.

77. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу : навч. посіб. – Київ : КНТ, 2011. – 260 с.

78. Гурковський В. І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства / В. І. Гурковський // Правова інформатика. − 2010. − № 2(26). − С. 72−77.

79. Гусєв В. О. Державна інноваційна політика: методологія формування і впровадження : монографія / В. О. Гусєв. – Донецьк : Юго-Восток, 2011. – 624 с.

80. Гуцалюк М. Інформаційна безпека України: нові загрози / М. Гуцалюк // Бизнес и безопасность. − 2003. № 5. − С. 2−3.

81. Давос, Швейцария. 11.01.2006 г. [Электронный ресурс]. – Режим доступа : http://www.distribut.net/global.shtml.

82. Дайзард У. Наступление информационного века. Новая технократическая волна на Западе / У. Дайзард. – М. : Наука, 1988. – 218 с.

83. Далворт М. Социальные сети: руководство по эксплуатации / Майк Далворт ; [пер. с англ. О. Петрова]– М. : Добрая книга, 2010.– 248 с.

84. Данільян О. Г. Національна безпека України: сутність, структура та напрями реалізації / О. Г. Данільян, О. П. Дзьобань, М. І. Панов. – Харків : Фоліо, 2010. − 296 с.

85. Данилова А. А. Манипулирование словом в средствах массовой информации / А. А. Данилова. – М. : Добросвет ; Киев : КДУ, 2009. – 234 с.

86. Діденко Н. Г. Управління, влада, держава: філософські аспекти взаємодії : монографія / Н. Г. Діденко. – Донецьк : ДонДУУ, 2005. – 128 с.

87. Дилтс Р. Изменение убеждений с помощью НЛП / Р. Дилтс. М. : Класс, 1997. – 192 с.

88. Державна політика: аналіз та механізм її впровадження в Україні : навч. посіб. / кол. авт. ; за заг. ред. В. А. Ребкала, В. В. Тертички. – Київ : УАДУ, 2000. – 232 с.

89. Державне регулювання економіки : навч. посіб. / С. М. Чистов, А. Є. Никифоров, Т. Ф. Куценко. – Київ : КНЕУ, 2005. – 440 с.

90. Державне управління : навч. посіб. / А. Ф. Мельник, О. Ю. Оболенський, А. Ю. Васіна ; за заг. ред. А. Ф. Мельник. – Київ : Знання, 2009. – 582 с.

91. Державне управління : словник-довідник / заг. ред. В. М. Князєв, В. Д. Бакуменко. – Київ : Видавництво УАДУ, 2002. – 228 с.

92. Державне управління в Україні : навч. посіб. / за заг. ред. В. Б. Авер'янова. – Київ : Юрінком Інтер, 1998. – 432 с.

93. Державне управління в Україні: наукові, правові, кадрові та організаційні засади : навч. посіб. / за заг. ред. Н. Р. Нижника, В. М. Олуйка. – Львів : Вид-во Національного університету «Львівська політехніка», 2002. – 352 с.

94. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки / В. Н. Дереко // Інформаційна безпека людини, суспільства, держави. − 2015. − № 2 (18). − С. 16−22.

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

96. Дмитрачков И. В. Информационно-коммуникативное обеспечение государственного управления в контексте политической модернизации : автореф. дис. ... канд. полит. наук / И. В. Дмитрачков. – М., 2008. – 20 с.

97. Довгань О. Д. Сучасні інформаційні структури як компоненти інформаційної безпеки / О. Д. Довгань // Інформація і право. 2015. − № 2(14). − С. 111−120.

98. Довгань О. Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки / О. Д. Довгань // Інформація і право. – 2012. − № 3(12). − С.102−112.

99. Довгань О. Д. Нейтралізація міжнародних інформаційних загроз / О. Д. Довгань // Правова інформатика. – 2014. − № 2(42). − С.80−89.

100. Додин И. С. Информационно-коммуникационные технологии в системе государственного управления регионом : автореф. дис. ... канд. полит. наук. – Саратов, 2007. – 20 с.

101. Домарев В. В. Безопасность информационных технологий. Методы создания систем защиты / В. В. Долмарев. − Київ : ООО ТИД ДС, 2001. − 688 с.

102. Домарев В. В. Защита информации и безопасность компьютерных систем / В. В. Долмарев. – Киев : Диа-Софт, 1999. – 480 с.

103. Домбровська С. М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України / С. М. Домбровська // Теорія та практика державного управління. − 2015. − Вип. 1 (48). − С. 2−4.

104. Домбровська С. М. Механізми формування безпеки держави [Електронний ресурс] / С. М. Домбровська, С. Т. Полторак // Теорія та практика державного управління і місцевого самоврядування. – 2015. – № 1. – Режим доступу: http://el-zbirn-du.at.ua.

105. Донченко О. Архетипи соціального життя і політика: монографія / О. Донченко, Ю. Романенко. – Київ : Либідь, 2001. – 334 с.

106. Древаль Ю. Д. Безпека особистості як фактор сучасних державно-управлінських відносин [Елеткронний ресурс] / Ю. Д. Древаль // Наукові записки Інституту законодавства Верховної Ради України. – С. 123–127. – Режим доступу: http://instzak.rada.gov.ua/instzak/doccatalog/document?id=72940.

107. Дубас О. П. Інформаційний розвиток сучасної України у світовому контексті : монографія. − Київ : Генеза, 2011. − 208 с.

108. Дурдинець В. Правова інформатика : підруч. / Є. Моісеєв, М. Швець ; за ред. В. Дурдинця. – Київ : ПанТот, 2010. – 524 с.

109. Жарков Я. М. Інформаційна безпека особистості, суспільства, держави : підручник / Я. М. Жарков. – Київ : Видавничо-поліграфічний цента «Київський університет», 2008. − 256 с.

110. Жарков Я. Інформаційно-психологічне протиборство в сучасному світі: проблемно-історичний аналіз / Я. Жарков, М. Онищук // Вісник Київського національного університету імені Тараса Шевченка. – 2007. – 14–15. – С. 101–104.

111. Жарков Я. Цілі, напрями проведення інформаційно-психологічних операцій / Я. М. Жарков, Л. М. Бєсєдіна // Збірник наукових

праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2008. – Вип. 16. С. 124–130.

112. Жатканбаева А. Е. Функциональные компоненты информационной безопасности / А. Е. Жатканбаева // Право и государство. − 2013. − № 4 (61). − С. 73−77.

113. Жданов І. Україні у XXI столітті: виклики для політичної еліти / І. Жданов, Ю. Якіменко // Національна безпека і оборона. – 2004. – № 9.– С. 2–30.

114. Иванов В. Ф. Аспекты массовой коммуникации : монография / В. Ф. Иванов. – Киев : ЦВП, 2009. – 190 с.

115. Исторические аспекты гибридной войны (в американском измерении) [Електронний ресурс] // Борисфен Интел [сайт]. – Режим доступа: http://bintel.com.ua/ru/article/10-AmericanHybridWar.

116. Захаренко К. В. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі / К. В. Захаренко // Гуманітарний вісник ЗДІА. − 2018. – Вип. 72. − С. 44−52.

117. Зернецька О. В. Глобальний розвиток систем масової комунікації і міжнародні відносини / О. В. Зернецька.– Київ : Освіта, 2002. – 351 с.

118. Золотар О. О. Загрози інформаційній безпеці людини / О. О. Золотар // Правова інформатика. – 2014. − № 2(42). − С.70−79.

119. Зубков С. А. Взаимосвязь политики, науки и техники в условиях техногенной цивилизации (социально-философские аспекты) : автореф. дис. ... д-ра филос. наук / С. А. Зубков. – М., 2006. – С. 15.

120. Иващенко Г. В. О понятии «безопасность» / Г. В. Иващенко // Credo. – Оренбург : Изд-во Оренбургского ун-та, 2000. – № 6. – С.52.

121. Іляш О. І. Трансформації системи соціальної безпеки України: регіональний вимір : монографія / О. І. Іляш. – Львів : Львівська комерційна академія, 2012. – 592 с.

122. Інтернет становить загрозу для інформаційної безпеки України [Електронний ресурс] // Телекритика (Звіт за підсумками круглого столу «Інформаційна безпека України. Медійний аспект», 30

вересня 2008 р.) [сайт]. Режим доступу: http://www.telekritika.ua/bezpeka/2008-10-24/41481.

123. Информационное общество: концепции и историческая практика / Е. В. Горелова // Вопросы культурологии. – 2007. – № 4. – С. 70–72.

124. Інформаційна безпека (соціально-правові аспекти) : підручник / В. Остроухов, В. Петрик, М. Присяжнюк та ін. ; за ред. Є. Д. Скулиша. Київ : КНТ, 2010. − 776 с.

125. Інформаційна політика : навч. посіб. / Г. Почепцов, С. Чукут. − Київ : Знання, 2008. − 663 с.

126. Інформаційне законодавство України : науково-практичний коментар / за ред. С. В. Бондаренко. – Київ : Юридична думка, 2009. – 241 с.

127. Кабінет Міністрів України : офіц. сайт [Електронний ресурс]. – Режим доступу : https://www.kmu.gov.ua.

128. Калиниченко Л. А. Методы и средства интеграции неоднородных баз данных / Л. А. Калиниченко – М. : Наука, 1983. – 420 с.

129. Калитич Г. І. Консолідація інформації, знань і мудрості як проектування і основа гармонійного поступу України / Г. І. Калитич // НТІ. – 2008. – № 1. – С. 51.

130. Канюков С. К. Информационно-культурологические аспекты теории национальной безопасности: опыт системного культурологического анализа : автореф. дис. ... канд. культуролог. наук / С. К. Канюков. – СПб., 1997. – 20 с.

131. Карнеги Д. Как приобретать друзей и оказывать влияние на людей / Д. Карнеги. – М. : Дом славянской книги, 2004. – 590 с.

132. Карнышев А. Д. Психология и технология политического соперничества / А. Д. Карнышев, К. С. Жуков, В. Ф. Шестак. – М. : ИМА-пресс, 2001. – 208 с.

133. Карпенко О. В. Механізми формування та реалізації сервісно-орієнтованої державної політики в Україні : автореф. дис. … д-ра н. з держ. упр. : спец. : 25.00.02 / О. В. Карпенко ; Нац. акад. держ. упр. при Президентові України. – Київ, 2016. – 37 с.

134. Кастельс М. Информационная эпоха: экономика, общество и культура / М. Кастельс. – М. : ГУ ВШЭ, 2000. – 395 с.

135. Катвалюк А.Л. Социальные технологии / А. Л. Катвалюк. – Тернополь: Экономична думка, 2001. – 284 с.

136. Кемаль А. Кибер война. как Россия манипулирует миром / А. Кемаль. – М. : Алгоритм, 2015. – 208 с.

137. Качинський А. Б. Індикатори національної безпеки: визначення та застосування їх граничних значень : монографія / А. Б. Качинський. – Київ : НІСД, 2013. – 101 с.

138. Киви Б. Гигабайты власти. Информационные технологии между свободой и тоталитаризмом / Б. Киви. – М. : Бестселлер, 2004. – 354 с.

139. Киссейн Э. Основы контентной стратегии / перв. англ. П.Миронов. – М. : Манн, Иванов и Фарбер, 2012. – 125 с.

140. Коваленко М. М. Компьютерні віруси і захист інформації / М. М. Коваленко. – К : Наукова думка, 1999. – 268 с.

141. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки / В. К. Конах // Стратегічні приоритети. – 2012. – № 3 (24). – С. 152−157.

142. Коньков Н. Война пятого поколения [Електронний ресурс] / Н.Коньков // Завтра [сайт]. – Режим доступу: http://www.zavtra.ru/content/view/2011-03-1543/

143. Концептуальні засади взаємодії політики й управління : навч. посіб. / Е. А. Афонін, Я. В. Бережний, О. Л. Валевський ; за заг. ред. В. А. Ребкала, В. А. Шахова, В. В. Голуб та ін. – Київ : НАДУ, 2010. – 299 с.

144. Коныk Д. Расставьте сети. Как использовать Интернет в интересах вашого бизнеса / Д. Коныk. С. Рендел. – Киев: ЛИК, 2011. – 120 с.

145. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посібник / Б. А. Кормич. – Київ : Кондор, 2004. – 384 с.

146. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія / Б. А. Кормич. – Одеса : Юридична література, 2007. – 471 с.

147. Корнейко О. Застосування та визначення терміна «інформаційна безпека» в національному законодавстві / О. Корнейко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. − 2009. − Вип. 2(19). − С. 9−13.

148. Корчагін М. Поняття інформації як цивільно-правової категорії [Електронний ресурс] / М. Корчагін. – Режим доступу : http://www.justinian.com.ua/article.php?id=2392.

149. Косарев В. М. Информационная безопасность: организация защиты програм и данных : учебное пособие / В. М. Косарев, А. Н. Петренко. – Днепропетровск : Изд-во ДУЭП, 2003. − 152 с.

150. Костенко Г. Ф. Теоретичні аспекти стратегії національної безпеки / Г. Ф. Костенко. – Київ : ДЕМІД, 2002. – 144 с.

151. Костюк В. І. Инфраструктура инноваций как основа перехода к информационному обществу / В. І. Костюк, Г. Л. Смолян, Д. С. Черешкин // Библиотека в эпоху перемен. – 2002. – № 1. – С. 60–75.

152. Котенко И. В. Перспективные направления исследований в области компьютерной безопасности / И. В. Котенко, Р. М. Юсупов // Защита информации. INSIDE. – 2006. – № 2. – С. 46−57.

153. Кохановська О. В. Правове регулювання у сфері інформаційних відносин : монографія / О. В. Кохановська. – Київ : Націон. акад. внутр. справ України, 2010. − 212 с.

154. Кравченко В. В. Національна стратегічна культура у політиці безпеки й оборони Франції / В. В. Кравченко // Гілея: науковий вісник. Збірник наукових праць. – 2010. – Випуск 34. – С. 174–178.

155. Кравченко И. И. Бытие политики / И. И. Кравченко. – М., 2001. – 259 с.

156. Кракович Д. Проигрывает ли Украина в информационной войне на своей территории? [Електронний ресурс] / Д. Кракович // Диалог.UA [сайт]. – Режим доступу: http://dialogs.org.ua/ru/project/page9802.html.

157. Красноступ Г. Проблема визначення об’єкта та предмета інформаційного права / Г. Красноступ // Право України. – 2011. – № 5. – С. 125−127.

158. Криштанович М. Ф. Реалізація механізмів публічного управління у сфері цивільного захисту України щодо національної безпеки / М. Ф. Криштанович // Вісник Національного університету цивільного захисту України. Серія. Державне управління. – 2017. – Вип. 1 (6). – С. 341–347.

159. Крюков О. І. Інформаційне забезпечення публічної влади як чинник національної безпеки держави в умовах глобалізації / О. І. Крюков // Вісник Національного університету цивільного захисту : зб. наук. праць. Серія: Державне управління. – Харків, 2016. – № 1 (4). – С. 142–149.

160. Кудрявцева С. П. Міжнародна інформація : навч. посіб. для студ. вищ. навч. закл. / С. П. Кудрявцева, В. В. Колос. − Київ : Слово, 2010. – 400 с.

161. Кунанець Н. Е. Консолідація інформації та інформаційна безпеку / Н. Е. Кунанець, В. В. Пасічник // ІІІ Міжнародна науково-практична конференція «Інформація та економічна безпеку (INFECO 2010)» : тези доповідей. − Харків : ДВНЗ УБС Харківський навчально-науковий інститут, 2010. − С. 131−133.

162. Курас І. Інтеграція інформаційних ресурсів – стратегічний напрям забезпечення інформаційних потреб суспільства / І. Курас // Бібліотечний вісник. – 2009. – №1. – С. 2−6.

163. Курбан О.В. Соціальні мережеві комунікаційні технології в структурі сучасних інформаційних потоків / О. В. Курбан // Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців. Матеріали ІІ Всеукраїнської наукової конференції (Львів, 25–26 жовтня 2013 р.). – Львів: Лігі-Прес, 2013. – С.137–143.

164. Курбан О. В. PR-аспекти інформаційної безпеки організаційних структур / О. В. Курбан // Вісник книжкової палати. – 2014. – №5. – С.48– 51.

165. Лешкевич Т. Г. Проблемы социокультурной самоидентификации в контексте коммуникации и глобализационных процессов / Т. Г. Лешкевич, Л. В. Евсеева // Межкультурный и межрелигиозный диалог в целях

устойчивого развития: материалы международной конференции, (Москва, 13– 16 сентября 2007 г.) / под общ. ред. В. К. Егорова. – М. : РАГС, 2008. – 848 с.

166. Лапин Н. И. Социальная информатика: основания, методы, перспективы / Н. И. Лапин. – М. ; Тюмень : Изд-во Тюмен. гос. ун-та, 2006. – 240 с.

167. Легасов В. А. Проблемы безопасного развития техносферы / В. А. Легасов // Энциклопедия / под ред. В. А. Пучкова. – М. : ФГБУ ВНИИ ГОЧС (ФЦ), 2015. – Т. 2: К–О. – 624 с.

168. Ленков С. В. Захист національних інформаційних ресурсів в аспекті інформаційної безпеки України / С. В. Ленков // Вісн. Східноукр. нац. ун-ту ім. В. Даля. – 2009. – Т. 1. − № 5. – С. 21−28.

169. Ліпкан В .А. Національна і міжнародна безпека у визначеннях та поняттях / В. А. Ліпкан, О. С. Ліпкан, О. О. Яковенко. − Київ : Текст, 2011. – 256 с.

170. Ліпкан В. А. Національна безпека України : навч. посіб. / В. А. Ліпкан. – Київ : КНТ, 2009. – 574 с.

171. Ливинская Н. Частные военные компании: вчера, сегодня, завтра / Н. Ливинская // Атташе. – 2007. – №2. – С. 96–103.

172. Лігачова Н. Телебачення спецоперацій / Н. Лігачова, С. Черненко, В. Іванов. – Київ : ТелеКритика, 2003. – 266 с.

173. Лисенко В. Чутки – активний засіб модифікації суспільної свідомості / В.Лисенко // Політичний менеджмент. – 2004. – № 6. – С. 96–102.

174. Лисичкин В. А. Третья мировая информационно-психологическая война / В. А. Лисичкин, Л. А. Шелепин. – М. : Академия социальных наук, 1999. – 207 с.

175. Луценко С. М. Особливості інформаційного забезпечення в державно-управлінській діяльності / С. М. Луценко // Держава та регіони : зб. наук. праць. – Запоріжжя : Класичний приватний університет, 2010. – № 2. – С. 41–45. – (Серія: «Державне управління»).

176. Мадера А. Г. Риски и шансы: неопределенность, прогнозирование и оценка / А. Г. Мадера. – М. : УРСС, 2014. – 448 с.

177. Макаренко Є. А. Європейська інформаційна політика : монографія. − Київ : Наша культура і наука, 2010. − 368 с.

178. Макаренко Є. А. Міжнародні інформаційні відносини : навч. посібник / Є. А. Макаренко. – Київ : Наша культура і наука, 2003. – 368 с.

179. Малик Я. Національна безпека : навч. посіб. / Я. Малик, О. Береза, М. Криштанович ; Львів. регіон. ін-т держ. упр. Нац. акад. держ. упр. при Президентові України. – Львів : ЛРІДУ НАДУ, 2010. – 280 с.

180. Мамаев М. Технологии защиты информации в Интернете : специальный справочник / М. Мамаев. – СПб : Питер, 2002. – 848 с.

181. Манойло А. Государственная информационная політика в особых условиях / А. В. Манойло. – М. : МИФИ, 2003. – С.18.

182. Манойло А. Государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. − М. : Горячая линия – Телеком, 2009. − 541 с.

183. Маракова І. Захист інформації : підручник для вищих навчальних закладів / І. Маракова, А. Рибак, Ю. Ямпольский. – Одеса : Одеський держ. політехнічний ун-т ; Ін-т радіоелектроніки і телекомунікаці, 2001. − 164 с.

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

185. Маруненко О. Зовнішні і внутрішні інформаційні війни у медійному просторі України / Олександр Маруненко // Освіта регіону. Політологія, психологія, комунікації. Український науковий журнал. – 2011.– № 4. – С. 92.

186. Марущак А. І. Інформаційне право : регулювання інформаційної діяльності : навч. посібник / А. І. Марущак. − Київ : Видавничий дім «Скіф», КНТ, 2010. − 344 с.

187. Марущак А. І. Правові основи захисту інформації з обмеженим доступом : курс лекцій / А. І. Марущак – Київ : КНТ, 2007. – 208 с.

188. Марчук Ю. Ескіз технології перетворення інформаційного потенціалу в інформаційний ресурс / Ю. Марчук // Вісн. Кн. палати. – 2005. – №1. – С.19−22.

189. Масляниця Й. У. Інформаційні ресурси України: проблеми державного управління : монографія / Й. У. Масляниця, О. В. Соснін, Л. Є. Шиманський. – Київ : НІСД, 2002. – 141 с.

190. Маслянко П. П. Інформаційні ресурси та засоби їх створення / П. П.Маслянко // Вісн. Східноукр. нац. ун-ту ім. В.Даля. – 2008. – Т.1. − № 7. – С. 132−140.

191. Мастяниця Й. У. Інформаційні ресурси України: проблеми державного управління : монографія / Й. У. Мастяниця. − Київ : НІСД, 2002. − 141 с.

192. Мишенин А. И. Теории экономических информационных систем / А. И. Мишенин. − М. : Финансы и статистика, 2002. −240 с.

193. Міністерство аграрної політики та продовольства України : офіц. сайт [Електронний ресурс]. – Режим доступу : https://agro.me.gov.ua/ua.

194. Міністерство внутрішніх справ України : офіційний сайт [Електронний ресурс]. – Режим доступу : https://mvs.gov.ua.

195. Міністерство енергетики та вугільної промисловості України : офіц. сайт [Електронний ресурс]. – Режим доступу : http://mpe.kmu.gov.ua.

196. Міністерство енергетики та захисту довкілля України : офіц. сайт [Електронний ресурс]. – Режим доступу : https://menr.gov.ua.

197. Міністерство закордонних справ України : офіц. сайт [Електронний ресурс]. – Режим доступу : https://mfa.gov.ua.

198. Міністерство інфраструктури України : офіц. сайт [Електронний ресурс]. – Режим доступу : https://mtu.gov.ua.

199. Міністерство культури і туризму України : офіц. сайт [Електронний ресурс]. – Режим доступу : http://mincult.kmu.gov.ua.

200. Міністерство молоді та спорту України : офіц. сайт [Електронний ресурс]. – Режим доступу : http://dsmsu.gov.ua/index/ua.

201. Міністерство оборони України : офіц. сайт [Електронний ресурс]. – Режим доступу : https://www.mil.gov.ua.

202. Міністерство освіти і науки України : офіц. сайт [Електронний ресурс]. – Режим доступу : https://mon.gov.ua/ua.

203. Міністерство охорони здоров’я України : офіц. сайт[Електронний ресурс]. – Режим доступу : https://moz.gov.ua.

204. Міністерство розвитку економіки, торгівлі та сільського господарства України : офіц. сайт[Електронний ресурс]. – Режим доступу : https://www.me.gov.ua.

205. Міністерство соціальної політики України : офіц. сайт [Електронний ресурс]. – Режим доступу : https://www.msp.gov.ua.

206. Міністерство фінансів України : офіц. сайт [Електронний ресурс]. – Режим доступу : https://mof.gov.ua.

207. Міністерство юстиції України : офіц. сайт [Електронний ресурс]. – Режим доступу : https://minjust.gov.ua.

208. Момот А. Аналіз основних напрямків забезпечення інформаційної безпеки / А. Момот // Актуальні проблеми міжнародних відносин. – 2008. – Вип. 659 (Ч.1). − №1. – С. 265−278.

209. Морозов И. Глобальные кибернетические системы как фактор безопасности демократического транзита [Электронный ресурс] / И. Морозов. – Режим доступа : http: //morozov. vi z. ru/library/bezo. Htm.

210. Музыка О. А. Ценностно-оценочный фактор в контексте социосинергетической парадигмы / О. А. Музыка. – Ростов н/Д. : Изд-во Рост. ун-та, 2006. – 240 с.

211. Мухин Г. В. Проблема обеспечения национальной безопасности в современных условиях / Г. В. Мухин. – М. : ВАХТ, 1994. – С. 27.

212. Негодаев И. А. На путях к информационному обществу / И. А. Негодаев. – Ростов н/Д. : Изд-во ДГТУ, 1999. – 246 с.

213. Нисневич Ю. Инфомация и власть / Ю. Нисневич. – М. : Мысль, 2000. – 175 с.

214. Нижник Н. Государственно-управленческие отношения в демократическом обществе / Н.Нижник. – Київ : Институт государства и права НАН Украины, 1995. – 207 с.

215. Нестеренко О. В. Єдина державна система електронних інформаційних ресурсів / О. В. Нестеренко // Науково-технічна інформація. – 2006. – № 4. – С. 3−9.

216. Общая теория национальной безопасности / под общ. ред. А. А. Прохожева. – М. : Изд-во РАГС, 2005. – 344 с.

217. Ожеван М. А. Основні напрями зовнішніх інформаційно-маніпулятивних впливів на суспільні трансформації в Україні: засоби протидії / М. А. Ожеван // Стратегічні пріоритети. – 2011. – № 3. – С. 118–126.

222. Окинавская хартия глобального информационного общества (Окинава, 22 июля 2000 г.) [Электронный ресурс]. – Режим доступа : https://zakon.rada.gov.ua

218. Олейников Е. Экономическая и национальная безопасность / Е. Олейников. – М., 2005. – 253 с.

219. Олійник О. В. Державна політика інформаційної безпеки України / О. В. Олійник // Юридичний вісник. − 2012. − №4(25). − С.65−69.

220. Орлов П. І. Інформатизація та інформація: нормативно-правове забезпечення : науково-практичний посібник / П. І. Орлов. – Харків : Харк. нац. ун-т внутр. справ, 2007. – 724 с.

221. Отчет Американской ассоциации информационных технологий (1TAA) [Электронный ресурс]. – Режим доступа : https://www.google.com/search?biw=914&bih=404&sxsrf=ACYBGNTEshcS4U2ayygCZZU10fgvo7ypIg%3A1571221829455&ei=RfGmXa-wiz.QloFKfdtIUk&ved=0ahUKEwjv64e4yaDlAhWbxMQBHbnOAosQ4dUDCAs.

222. Панарин И. Информационная война и власть / И. Н. Панарин. – М. : Мир безопасности, 2001. – С. 40.

223. Панарин И. Технология информационной войны : монография / И. Панарин. − М. : КСП+, 2003. − 320 с.

224. Партико З. В. Теорія масової інформації та комунікації / З. В. Партико. – Львів : Афіша, 2008. – 290 с.

225. Пархоменко В. Д. Наукові і організаційні проблеми управління інформаційними ресурсами / В. Д. Пархоменко // Науково-технічна інформація. – 2007. – № 3. – С. 31−36.

226. Петров А. А. Компьютерная безопасность. криптографические методы защиты / А. А. Петров. − М. : ДМК, 2000. − 448 с.

227. Пилипенко О. Формула безопасности : информационная безопасность / О. Пилипенко // СНІР. − 2005. − № 12. − С. 72−73.

228. Пилипчук В. Г. Еволюція наукових поглядів стосовно поняття «державна безпека» / В. Г. Пилипчук // Стратегічна панорама. – 2006. – № 2. – С. 17−21.

229. Пирожков С. І. Національна та регіональна безпека: погляд України / С. І. Пірожков // Нова безпека. – 2003. – №2. – С. 9–16.

230. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко // Сучасний захист інформації. − 2015. − № 4. − С. 86−90.

231. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення / В. С. Політанський // Науковий вісник Ужгородського національного університету. – 2017. – Вип. 42. − С. 16−22. – (серія «Право»).

232. Полюбина И. Б. Электронное правительство как составляющая новой экономики [Электронный ресурс] / И. Б. Полюбина. – Режим доступа : http://www.dofa.ru/ 5Шс1еп1/5еттаг/ро]иЬта.с1ос.

233. Пономарева Е. Г. Современная Россия: политические отношения и политические институты / Е. Г. Пономарева. – М. : МГИМО, 2006. – 302 с.

234. Попов В. Д. Информационная политика / В. Д. Попов. − М. : Изд-во РАГС, 2003. − 463 с.

235. Порфирьев Б. Н. Системная концепция национальной безопасности / Б. Н. Порфирьев. – М., 1995. – С. 11.

236. Почепко В. В. Очерки о власти: новые подходы и интерпретации. Раздел 1 / В. В. Почепко, Р. А. Хомелева. – СПб., 1998. – 464 с.

237. Почепцов Г. Інформаційна політика : навч. посіб. / Г. Почепцов, С. Чукут. – 2-е вид., стер. – Київ : Знання, 2008. – 663 с.

238. Почепцов Г. Теорія комунікації / Г. Почепцов. – Київ : Вид. центр «Київський університет», 1999. – 308 с.

239. Проданюк Р. І. Інформаційна безпека в соціологічному контексті: до постановки проблеми / Р. І. Проданюк // Грані : науково-теоретичний альманах. − 2018. − Т. 21. − № 4. − С. 84−90.

240. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314.

241. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851 // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.

242. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

243. Прокоф'єва Д. М. Інформаційна війна та інформаційна злочинність / Д. В. Прокоф'єва // Вісник Запорізького юридичного інституту. − 2000. − №1. − С. 288−307.

244. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

245. Про Національну програму інформатизації : Закон України від 04.02.1998 р. № 74 // Відомості Верховної Ради України. – 1998. – № 27. – Ст. 181.

246. Про основи національної безпеки України [Електронний ресурс] : Закон України від 19.06.2003 № 964-IV // БД «Законодавство України» / ВР України. – Режим доступу: http://zakon.rada.gov.ua/laws/show/964-15.

247. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. // Відомості верховної влади України. – 2007. – № 12. – Ст. 102.

248. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017 [Електронний ресурс] /

Офіц. сайт Президента України. – Режим доступу : https://www.president.gov.ua/documents/472017-21374.

249. Про Стратегію сталого розвитку «Україна – 2020» [Електронний ресурс] : Указ Президента Українивід 12.01.2015 р. № 5/2015. – Режим доступу: http://zakon.rada.gov.ua/laws/show/5/2015.

250. Рада національної безпеки і оборони України : офіц. Сайт [Електронний ресурс]. – Режим доступу : https://www.rnbo.gov.ua.

251. Размєтаєва Ю. С. Приватність в інформаційному суспільстві: проблеми правового розуміння та регулювання / Ю. С. Размєтаєва // Науковий вісник Ужгородського національного університету. – 2016. – Вип. 37. – Т. 1. − С. 43−46. – (Серія: Право).

252. Рождественська О. С. Особливий суб’єкт інформаційних правовідносин (загальнотеоретичний аспект) : дис. … канд. юрид. наук : 12.00.01 / О. С. Рождественська. – Харків, 2009. − 203 с.

253. Романов А. А. Массовые коммуникации : учебно-практическое пособие / А. А. Романов. – М. : Евразийский открытый институт, 2010. – 175 с.

254. Рубанець О. М. Інформаційне суспільство: когнітивний креатин постнекласичних досліджень : монографія / О. М. Рубанець. – Київ : Парапан, 2006. – 420 с.

255. Саркисян Д. Б. Международное сотрудничество по формированию глобального информационного общества / Д. Б. Саркисян // Научно-техническая информация. – 2007. – № 9. – С. 26−33. – (Серия «Организация и методика информационной работы»).

256. Сенченко О. П. Стратегія побудови та розвитку інформаційного суспільства / О. П. Сенчеко // Перспективи. – 2008. – № 2. – С. 8−19. – (Серія : філософія, історія, соціологія, політологія).

257. Серебрянников В. В. Безопасность России и Армия / В. В. Серебрянников, Ю. И. Дерюгин, Н. Н. Ефимов, В. И. Ковалев. – М. : Ин-т СПИ РАН, 1995. – 423 с.

258. Ситник Н. П. Влияние информации на человека / Н. П. Ситник // Науч. и техн. библиотеки. – 2004. – № 8. – С. 81−84.

259. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. / В. С. Сідак, В. Ю. Артемов. – Київ : КНТ, 2010. – 160 с.

260. Сілкова Г. Інформаційно-аналітичні дослідження в структурі інформаційних ресурсів / Г. Сілкова // Вісн. Кн. палати. – 2005. – № 2. – С. 14−18.

261. Сморгунов Л. В. Электронное правительство в контексте современных политических реформ на Западе [Электронный ресурс] / Л. В. Сморгунов. – Режим доступа : http://conf.infosoc.rn/03-rGOVfl4.html.

262. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету 2010. – № 2. – Т. 2. – С.32−35. – (Серія: Економічні науки).

263. Соціально-правові основи інформаційної безпеки : навч. посіб. / В. М. Петрик, А. М. Кузьменко, В. В. Остроухов та ін. ; за ред. В. В. Остроухова. – Київ : Росава, 2007. – 496 с.

264. Стратегия национальной безопасности США / пер. с англ. – М. : ОВПИ ВУ, 1995. – С. 8.

265. Степанов В. Ю. Сучасний інформаційний простір: особливості та тенденції розвитку : монографія / В. Ю. Степанов. – Харків : САМ, 2010. – 280 с.

266. Степанов В. Державна інформаційна політика: проблеми та перспективи : [монографія] / В. Степанов. – Харків : С.А.М. , 2011. – 548 с.

267. Степанова О. М. Інформаційна безпека в умовах розвитку інформаційної системи підприємства. / О. М. Степанова, Л. М. Дегтярьова // Інформаційна безпека. – 2009. −№ 1. – С. 59−63.

268. Столбовський А. Нові інформаційні технології та економічна безпека України / А. Столбовський // Актуальні проблеми економіки. – 2004. – № 8. – С. 99– 105.

269. Стратегія національної безпеки України : Указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. – Режим доступу : www.mig.com.ua/.../6021-poroshenko-utverdil-strategiyu-natsionalnoj-bez.

270. Тапскотт Д. Электронно-цифровое общество: плюсы и минусы эпохи сетевого интеллекта / Д. Тапскотт. – М. ; Киев, 1999.

271. Теория политики / под ред. Б. А. Исаева. – СПб. : Питер Пресс, 2007. – 464 с.

272. Термінологічний довідник з питань технічного захисту інформації / С. Р. Коженевський, Г. В. Кузнецов, В. О. Хорошко, Д. В. Чирков ; за ред. проф. В. О. Хорошка. – Київ : ДУІКТ, 2007. – 365 с.

273. Тертичка В. Державна політика: аналіз та здійснення в Україні / В. Тертичка. – Київ : Основи, 2002. – 750 с.

274. Ткачук Т. Ю. Конкурентна розвідка : монографія / Т. Ю. Ткачук. − Коломия : Коломийська друкарня ім. Шухевича, 2015. − 296 с.

275. Ткачук Т. Ю. Організаційне проектування у системі захисту конфіденційної інформації суб'єктів господарювання / Т. Ю. Ткачук, В. І. Журавель // Інформаційна безпека людини, суспільства, держави. − 2014. − № 1. − С. 76–84.

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

277. Торічний В. Державне управління у сфері боротьби з комп'ютерними злочинами як напрям забезпечення національної безпеки й охорони громадського порядку / В. Торічний // Забезпечення діяльності складових сектору безпеки і оборони України : тези міжнар. наук.-практ. конф. − Хмельницький : Вид-во НАДПСУ, 2019. − С. 574–575.

278. Торічний В. О. Державні механізми забезпечення корпоративної інформаційної культури [Електронний ресурс] / В. О. Торічний, В. О. Шведун // Державно-управлінські студії. − 2019. − №1 (12). – Режим доступу : http://studio.ipk.edu.ua/wp-content/uploads/2020/02/Borovs-ka-7.pdf

279. Торічний В. О. Державний функціональний комплекс забезпечення інформаційної безпеки на прикладі ветеринарного нагляду і контролю / В. О. Торічний, В. О. Шведун // Публічне управління і адміністрування в Україні. − 2020. − Вип. 15. − С. 118–121.

280. Торічний В. О. Дослідження методів оцінки результативності державної інформаційної політики у контексті забезпечення державної безпеки / В. О. Торічний // Держава та регіони. −2019. № 3 (67). − С. 200–203. − (Серія «Державне управління»).

281. Торічний В. О. Дослідження пропаганди як інструменту інформаційного забезпечення державної безпеки / В. О. Торічний // Право та державне управління. − 2019. − № 3 (36). − Т. 2. − С. 183–186.

282. Торічний В. О. Дослідження суперечностей у системі інформаційного забезпечення державної безпеки соціуму в умовах функціонування цифрового суспільства / В. О. Торічний // Актуальні проблеми економіки, управління та фінансів : матеріали міжнар. наук.-практ. конф. − Дніпро : Університет митної справи та фінансів, 2019. − С. 141–143.

283. Торічний В. О. Застосування інформаційно-комунікаційних технологій при реалізації освіти протягом життя [Електронний ресурс] / В. О. Торічний // Інноваційні технології розвитку особистісно-професійної компетентності педагогів в умовах післядипломної освіти : матеріали ІІІ Всеукр. наук.-практ. інтернет-конф. − Суми : Сумський обласний інститут післядипломної педагогічної освіти, 2019. – Режим доступу : https://drive.google.com/file/d/1kyurQfLDyMbzXusWvuzpKw5Nnanog2Hc/view

284. Торічний В. О. Інформаційна безпека як чинник функціонування сучасної держави в контексті формування суспільства знань / В. О. Торічний // Формування громадянської культури в новій українській школі: традиційні та інноваційні практики : матеріали ІІ Всеукр. наук.-практ. конф. − Суми : Сумський обласний інститут післядипломної педагогічної освіти, 2019. − С. 254–256.

285. Торічний В. О. Інформаційне забезпечення безпеки держави в умовах інформаційного суспільства: державно-управлінський аспект : монографія / В. О. Торічний. − Харків : НУЦЗУ, 2020. − 274 с.

286. Торічний В. О. Інформаційне забезпечення безпеки держави в контексті використання комп’ютерних технологій: державно-управлінський аспект / В. О. Торічний // Актуальні проблеми державного управління. − 2019. − № 2 (56). − С. 39–46.

287. Торічний В. О. Інформаційне забезпечення державної політики як найважливіший фактор безпеки держави / В. О. Торічний // Актуальні проблеми державного управління. − 2019. − № 1 (55). − С. 77–85.

288. Торічний В. О. Критерії та умови ефективності впровадження механізму реалізації державної інформаційної політики / В. О. Торічний // Державне управління у сфері цивільного захисту: наука, освіта, практика : матеріали міжнар. наук.-практ. конф. інтернет-конф. − Харків : Вид-во НУЦЗУ, 2020. − С. 80–81.

289. Торічний В. О. Необхідність створення і розвитку державної системи інформаційної безпеки: впровадження європейського досвіду дослідження впливових факторів / В. О. Торічний // Актуальні проблеми європейської та євроатлантичної інтеграції України : матеріали 16-ої регіон. наук.-практ. конф. − Дніпро : ДРІДУ НАДУ, 2019. − С. 229–230.

290. Торічний В. О. Основні функції та принципи інформаційного забезпечення держави [Електронний ресурс] / В. О. Торічний // Державно-управлінські студії. − 2018. − № 8 (10). – Режим доступу : http://box5800.temp.domains/~ipkeduua/

291. Торічний В. О. Особливості побудови державної системи інформаційної безпеки / В. О. Торічний // Вчені записки Таврійського національного університету ім. В. І. Вернадського. − 2019. − Т. 30 (69). − № 3. − С. 180–182.

292. Торічний В. О. Особливості державного управління регіональними системами інформаційної безпеки / В. О. Торічний // Публічне управління і адміністрування в Україні. − 2019. − № 11. − С. 183–185.

293. Торічний В. О. Проблема інформаційної безпеки в умовах розвитку інформаційного суспільства / В. О. Торічний // Теорія та практика державного управління. − 2019. − № 2 (65). − С. 256–262.

294. Торічний В. О. Процеси інформатизації державно-управлінських відносин та їх вплив на безпеку держави / В. О. Торічний // Теорія та практика державного управління. − 2019. − № 4 (67). − С. 179–187.

295. Торічний В. О. Процеси управління інформаційним забезпеченням соціальної безпеки в державі: особливості та вимоги / В. О. Торічний // Інформаційні технології: наука, техніка, технологія, здоров'я : тези доповідей XXVII наук.-практ. конф. MicroCAD-2019. Ч. IV. − Харків : НТУ «ХПІ», 2019. − С. 122.

296. Торічний В. О. Розробка інноваційних методів державного захисту територіального інформаційного простору / В. О. Торічний // Інноваційний розвиток і підвищення рівня спроможності об'єднаних територіальних громад : матеріали науково-практичної конференції за міжнародною участю. − Дніпро : ДРІДУ НАДУ, 2019. − С. 301–302.

297. Торічний В. О. Система інформаційного забезпечення державної безпеки України [Електронний ресурс] / В. О. Торічний // Державне будівництво. − 2020. − № 1. – Режим доступу : www.kbuapa.kharkov.ua/e-book/db/2020-1/index.html.

298. Торічний В. О. Стратегічні орієнтири інформаційного забезпечення державної безпеки України [Електронний ресурс] / В. О. Торічний // Державне управління: удосконалення та розвиток. − 2019. − № 11. – Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=1711.

299. Торічний В. О. Технології формування та реалізації інформаційної політики держави / В. О. Торічний // Вісник Національного університету цивільного захисту України. − 2019. − Вип. 2 (11). − С. 201–207. − (Серія «Державне управління»).

300. Торічний В. О. Умови ефективної розробки та впровадження державної інформаційної політики / В. О. Торічний // Публічне управління та митне адміністрування. − 2020. − № 2 (25). − С. 50–62.

301. Торічний В. О. Формування та впровадження державної інформаційної політики як запорука забезпечення державної безпеки / В. О. Торічний // Вісник Національного університету цивільного захисту України. − 2019. − Вип. 1 (10). − С. 64–69. − (Серія «Державне управління»).

302. Торічний В. О. Формування та реалізація єдиної державної політики у сфері інформаційної безпеки / В. О. Торічний // Державне управління у сфері цивільного захисту: наука, освіта, практика : матеріали міжнар. наук.-практ. конф. − Харків : Вид-во НУЦЗУ, 2019. − С. 112–113.

303. Торічний В. О. Шляхи підвищення інформаційної безпеки на державному рівні / В. О. Торічний // Інформаційні технології: наука, техніка, технологія, здоров'я : тези доп. XXVIII наук.-практ. конф. MicroCAD-2020. Ч. V. − Харків : НТУ «ХПІ», 2020. − С. 128–129.

304. Тоффлер Э. Метаморфозы власти / Э. Тоффлер ; пер. с англ. – М. : АСТ, 2003. – С.46.

305. Уэбстер Ф. Теории информационного общества / Ф. Уэбстер ; пер. с. англ. М. В. Арапова ; под ред. И. В. Маныхиной. – М. : Аспект-Пресс, 2004.– 400 с.

306. Хакен Г. Информация и самоорганизация / Г. Хакен. – М., 2001.

307. Халипов В. Ф. Энциклопедия власти / В. Ф. Халипов. – М. : Академический Проект ; Культура, 2005. – 1054 с.

308. Харари Ю. 21 урок для XXI века / Ю. Харари. – М. : Синдбад, 2019. – 246 с.

309. 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.

310. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності / Р. М. Хмелевський // Сучасний захист інформації. − 2016. − № 4. − С. 65−70.

311. Хорошко В. О. Основи інформаційної безпеки / В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест; за ред. проф. В. О. Хорошка. – Київ : ДУІКТ, 2008. – 186 с.

312. Хромченко Л. Г. Теоретические основы организации информационной деятельности / Л. Г. Хромченко, С. М. Панин. – Харьков ; Симферополь : МСУ, СВА МСУ, 2004.– 503 с.

313. Философский энциклопедический словарь. – М. : Сов. энциклопедия, 1983. – С. 214.

314. Федоров А. В. Информационная безопасность в мировом политическом процессе / А. В. Федоров. – М. : МГИМО, 2006. – 218 с.

315. Цаленко М. Ш. Основы теории информационных ресурсов и социальная память / М. Ш. Цаленко // Научно-техническая информация. – 2006. – № 12. – С.1−11. – (Серия : «Организация и методика информационной работы»).

316. Царегородский А. В. Информационная безопасность в распределенных управляющих системах : монография / А. В. Царегородский. – М. : Изд-во РУДН, 2003. − 217 с.

317. Цимбалюк В. С. Основи інформаційного права України : навч. посіб / В. С. Цимбалюк, В. Д. Гавловський, В. В. Грищенко та ін. ; за ред. М. Я. Швеця, Р. А. Калюжного та П. В. Мельника. – Київ : Знання, 2010. – 274 с.

318. Чернов А. А. Становление глобального информационного общества: проблемы и перспективы / А. А. Чернов. – М. : Дашков и К°, 2003. – 232 с.

319. Чиж І. С. Україна: шлях до інформаційного суспільства / І. С. Чиж.– Київ : Либідь, 2005. – 119 с.

320. Шайгородський Ю. Ціннісні трансформації в період суспільних змін // Ю. Шайгородський // Соціальна психологія – 2009. – № 3. – С. 86–86.

321. Шамхалов Ф. Основы теории государственного управления / Феликс Шамхалов. – М. : Экономика, 2003. – 518 с.

322. Шаповал Р. В. Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України / Р. В. Шаповал, В. О. Клочко // Наше право. − 2014. − № 6. − С. 5−9.

323. Шварценберг Р.-Ж. Политическая социология. / Роже-Жерар Шварценберг. / [Пер. с фр.] – В 3 ч. – Ч.1 – М. : Б.и., 1992. – 180 с

324. Шемшученко Ю. С. Інформаційне законодавство України : науково-практичний коментар / За ред. Ю. С. Шемшученка, І. С. Чижа. – Київ : Юридична думка, 2011. − 232 с.

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

326. Шеннон К. Математическая теория связи / К. Шеннон // Работы по теории информации и кибернетике. – М. : ИЛ, 1963. – С. 243–332.

327. Шпакова О. Политика информационной безопасности в Украине: правовой базис / О. Шпакова // Актуальні проблеми міжнародних відносин. − 2008. – Вип. 65 (Ч. 1). − С. 242−249.

328. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ / В. М. Щербина // Актуальні проблеми економіки. − 2006. − № 10. − С. 220−225.

329. Юдін О. К. Інформаційна безпека держави : навч. посіб. / О. К. Юдін, В. М. Богуш. − Харків : Консул, 2011. − 576 с.

330. Яковенко В. Я. Інформаційні ресурси : навч. посіб. / В. Я. Яковенко. – Донецьк : Дон Ну, 2005. – 202 с.

331. Яковенко М. Інформаційний простір: філософські аспекти формування поняття / М. Яковенко // Вісник. – Львів, 2011. – № 692: Філософські науки. – С. 22–27.

332. Янков М. Материя и информация / М. Янков. – М. : Прогресс, 1979. – С. 334.

333. Ярема О. Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві / О. Г. Ярема // Науковий вісник Львівського державного університету внутрішніх справ. – 2016. − № 2. − С. 244−252. – (Серія: «Право»).

334. Ярочкин В. И. Безопасность информационных систем / В. И. Ярочкин. – М. : ОСЬ–89, 1996. – 320 с.

335. Яшин Б. Л. Культура общения: теория и практика коммуникаций : учебное пособие. – М. : Директ-медиа, 215. – 243 с.

336. Almond G. The Intellectual History of Civic Culture Concept. The Civic Culture Revisited // Gen. Editors G. Almond, S. Verba – Boston. – Toronto, 1980. – P. 1–36.

337. Arnstein S. A ladder of citizen participation in the USA // Journal of the Royal Town Planning Institute, vol. 57, no. 4, pp. 176–182.

338. Bell D. The Social Famework of the Information Society / D. Bell. – Oxford, 1980.

339. Castells M. The Information Age: Economy, Society and Culture: End of Milenium. Maiden (Ma.) / M. Castells. – Oxford : Blackwell Publ., 1998.

340. Citizens and the New Governance. Beyond New Public Management / Edited by Luc Rouban. – IOS Press, Ohmsha, 1997. – 237 p.

341. Crozier M. La Société bloquée / M. Crozier. – Paris, 1971. – 253 p.

342. Dahl R. Development and Democratic Culture in Consolidating the Third Wave Democracies / Ed. by L. Diamond. – Baltimor; London, 1997. – 360 p.

343. Diamond L. Developing Democracy. Toward Consolidation. / L.Diamond – Baltimore ; London, 1999. – 612 p.

344. Dizard Wilson J. Old media, mass communications in the information age. – New York: Longman, 1994. – P. 215.

345. Eckstein H. Comparative Politics: A Reader. / H. Eckstein, D. E. Apter – N.Y. : Free Press, 1963.

346. Freedom in the World 2009 Survey Release // http://www.freedomhouse.org/template.cfm?page=445.

347. Goban-Klas'ом T. Media i komunikowanie masowe: Teorie i analizy prasy, radia, telewizji i Internetu. – Warszawa; Kraków: Wydawnictwo Naukowe PWN SA, 1999. – C. 52–79.

348. Habermas J. Legitimation Crisis. / J. Habermas – Boston, 1975.

349. Habermas J. The theory of communicative action. – Vol. 1 : Reason and the rationalization of society. – Cambridge, 1995.

350. Hundley R. O. The Global Course of the Information Revolution: Political, Economic and Social Conséquences / R. O. Hundley. – RAND, 2000. – P. 109.

351. Inkeles A. The Totalitarian Mystique: Some Impressions on the Dynamics of Totalitarian Society // Totalitarianism. – N.-Y., 1964. – P. 88 – 90.

352. Rogers Everett M. Diffusion of Innovations. 4thed. New York: Free Press,1995.

353. Rogers E. M., Shoemaker F. F. Communication of Innovations : a cross-cultural approach. 2nd ed. – New York, Free Press, 1971 – 476 p.

354. Landy F.G. Psychology of work behavior. Dorsey Press, 1985.

355. Lasswell H. The Structure and Function of Communication in Society // The Process and Effects of Mass Communication. Chicago, 1971.

356. Lasswell H. The Uses of Content Analysis Data in Studying Social Change // Science and Culture. 1967. Vol. 33. No 4.

357. Masuda Y. The Information Society as Postindustrial Society / Y. Masuda. – Wash. : World Future Soc., 1983. – P. 29.

358. McLuhan M. The medium is the message. – N. Y.: Springer, 1967. – P. 87–89.

359. McQuail D. Media Performance. Mass Communication and the Public Interest / D. McQuail. – London ; Newbury Park ; New Delhi : SAGE Publications, 1993. – 350 p.

360. Morgan Nick; Moshiri Farrokh. Management communication : an anthology San Diego, Calif. : Cognella, 2011. 350 p. : ill. ; 28 cm. ISBN: 9781609279257 1609279255

361. Nations in Transit – Ukraine (2008). – Режим доступу: http://www.freedomhouse.org/template.cfm?page=47&nit=472&year=2008

362. Nicole de Montricher. Citizens and the Quality of Public Action: Seeking a New Form of Management. Public Participation and Contracting Practices in France // Citizens and the new Governance. – Netherlands, 1999. – 239 pp.

363. O'Donnell G. Transition, Continuities, and Paradoxes. / G. O'Donnell // Issues in Democratic Consolidation: The New South American Democracies in Comparative Perspective / Ed. by Sc. Mainwaring, G. O'Donnell and J. S. Valenzuela. – Notre Dame, 1992.

364. Roszak T. The Cult of Information: The Folklore of Computers and the True Art of Thinking / T. Roszak. – New York : Pantheon Book, 1986. – P. 14.

365. Thomson, K.L., Von Solms, R., Louw, L. 2006. "Cultivating an organizational information security culture", Computer Fraud & Security, vol. 10, pp. 7-11.

366. Schwartzenberg R.-J. Sociology Politique / R.-J. Schwartzenberg. – P., 1988. – P. 42.

367. Verdasys. «Kill Chain» Defense is Critical Against Cyber Attacks that Steal Sensitive Data, Verdasys White Paper Says. – (2013). – URL: https://www.verdasys.com/news-events/press/cyber-defensewhitepaper-release-6june2013-final.pdf.

368. Von Solms R., Von Solms B. From policies to culture // Computers & Security. – 2000. – Vol. 23. – Issue 4. – P. 275–279.

369. Vroom C., von Solms R.. Towards information security behavioral compliance // Computers & Security. – 2003. – № 23 (1). – P. 191–198.

370. Whitman, M.E, Mattord, H.J 2012, Principles of Information Security, Course Technology, Boston.

ДОДАТКИ

Додаток А

Довідка про впровадження результатів дисертаційного дослідження

ДСНС України
ГОЛОВНЕ УПРАВЛІННЯ ДЕРЖАВНОЇ СЛУЖБИ УКРАЇНИ
З НАДЗВИЧАЙНИХ СИТУАЦІЙ У ХМЕЛЬНИЦЬКІЙ ОБЛАСТІ
(ГУ ДСНС України у Хмельницькій області)

вул. Героїв Чорнобиля, 1/2, м. Хмельницький, 29000, тел.: (0382) 65-65-53, факс (0382) 66-45-23
www.km.dsns.gov.ua код ЄДРПОУ 38662200 E-mail: odsokc@km.dsns.gov.ua

№ 01-1985/02 На № _____ від _____

ДОВІДКА
про використання результатів дисертаційного дослідження
Торічного Вадима Олександровича
«Інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів і загроз»

Результати дисертаційного дослідження Торічного В. О. знайшли відображення у практичній діяльності в контексті використання стратегії інформаційного забезпечення державної безпеки, яка орієнтована на передбачення умов для створення можливостей максимального впровадження інтелектуальних систем у процеси забезпечення державної безпеки.

На особливу увагу заслуговують пропозиції автора щодо створення єдиної державної системи моніторингу інформаційного простору, а також створення інформаційної системи та інфраструктури Оперативного центру забезпечення інформаційної безпеки.

У цілому, дисертаційне дослідження Торічного В. О. містить результати, що відіграють суттєву роль у процесах державного управління у сфері інформаційного забезпечення державної безпеки.

Начальник ГУ ДСНС України
у Хмельницькій області
генерал-майор служби цивільного захисту Едуард Братко

Додаток Б

Довідка про впровадження результатів дисертаційного дослідження

ХМЕЛЬНИЦЬКА МІСЬКА РАДА
ВИКОНАВЧИЙ КОМІТЕТ
вул. Гагаріна, 3, м. Хмельницький, 29000
тел (0382) 76-50-05, 76-50-86, факс 76-43-54
E-mail: rada@khm.gov.ua, http:// www.khm.gov.ua
Код ЄДРПОУ 04060772

від 13.05.2020 № 02-21-598
на № _____ від _____

ДОВІДКА

про використання результатів дисертаційного дослідження

Торічного Вадима Олександровича

«Інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів і загроз»

У дисертації Торічного В.О. вирішується актуальна науково-практична проблема, яка полягає в системному аналізі стану та перспектив національної безпеки держави в інформаційній сфері, а також у розробленні нових підходів до вирішення проблемних питань і підготовці науково-прикладних рекомендацій щодо формування та реалізації державної інформаційної політики держави в контексті національної безпеки.

Дисертаційне дослідження Торічного В.О. має практичну значущість стосовно створення інформаційно-комунікаційної архітектури органів місцевого самоврядування, яка дозволяє уніфікувати діяльність державних органів у регіонах за рахунок використання єдиних бізнес-процесів, шаблонів документів, стандартів і типових рішень в межах інформаційно-комунікаційних технологій.

На особливу увагу заслуговують запропоновані заходи щодо створення єдиного інформаційно-аналітичного середовища державних органів, як основного інструменту узгодженого проведення всіх видів реформ державного управління у сфері інформаційної безпеки.

Перспективність застосування висновків і пропозицій автора дисертаційного дослідження у практичній діяльності не викликає сумнівів враховуючи їх актуальність і змістовність.

Заступник міського голови Анатолій НЕСТЕРУК

Додаток В

Довідка про впровадження результатів дисертаційного дослідження

УКРАЇНА
ХМЕЛЬНИЦЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
ДЕПАРТАМЕНТ ОСВІТИ І НАУКИ
Будинок освіти, Майдан Незалежності, 1, м. Хмельницький, 29000,
тел./факс (0382) 79-51-36, E-mail: 39091603@mail.gov.ua, Web: http://osvita.adm-km.gov.ua,
код ЄДРПОУ 39091603

від 13.05.20 № 1189-41/2020

на № _____ від _____

ДОВІДКА
про використання результатів дисертаційного дослідження
Торічного Вадима Олександровича
“Інформаційне забезпечення державної безпеки України
в умовах трансформацйних викликів і загроз”

Практична значущість дисертаційного дослідження Торічного В.О. полягає у розробці та впровадженні комплексу заходів щодо формування Стратегії інформаційного забезпечення державної безпеки.

Зокрема, завдяки розробкам автора, в практичну діяльність було впроваджено елементи запропонованої національної Стратегії інформаційного забезпечення державної безпеки у контексті консолідації всіх верств суспільства для досягнення поставлених цілей інформаційного й інноваційного розвитку, а також координації бізнесу, всіх суспільних інститутів та громадян з метою інформаційного забезпечення національної безпеки.

Вищезазначене уможливлює прийняття раціональних рішень відносно формулювання регіональних пріоритетів інформаційного забезпечення національної безпеки, а також відносно попередження дії негативних чинників, що загрожують інформаційній безпеці країни.

У цілому, дисертаційне дослідження Торічного В.О. має суттєву практичну значущість та дозволяє вдосконалити процеси функціонування органів державної влади та місцевого самоврядування відносно підтримки належного рівня інформаційної безпеки в країні та регіонах.

Директор Департаменту _____ **Олег ФАСОЛЯ**

Додаток Г

Акт про впровадження результатів дисертаційного дослідження

ДЕРЖАВНА ПРИКОРДОННА СЛУЖБА УКРАЇНИ

Національна академія Державної прикордонної служби України імені Богдана Хмельницького

вул. Шевченка, 46, м. Хмельницький, 29000 тел. 79-59-11, факс 72-08-02, e-mail: nadpsu@dpsu.gov.ua

На № від _____ 2020 р. №_____
На №_____ від _____ 2020 р.

ЗАТВЕРДЖУЮ

Заступник ректора (проректор) Національної академії Державної прикордонної служби України імені Богдана Хмельницького з наукової роботи, доктор педагогічних наук,

полковник Сергій БІЛЯВЕЦЬ

«_____» _____ 2020 р.

АКТ

про реалізацію результатів наукового дослідження
ТОРІЧНОГО Вадима Олександровича
на тему: «Інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів та загроз» на здобуття наукового ступеня доктора наук з державного управління зі спеціальності 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку в освітньому процесі Національної академії Державної прикордонної служби України імені Богдана Хмельницького

Комісія у складі: голова комісії – професор кафедри прикордонної безпеки, доктор наук з державного управління, доцент Геннадій МАГАСЬ; члени комісії: головний науковий співробітник науково-дослідного відділу доктор наук з державного управління, професор Валерій ДОВГАНЬ; начальник кафедри національної безпеки (сфера прикордонної діяльності) та управління, доктор військових наук, доцент, полковник Юрій ІВАШКОВ; начальник навчального відділу, кандидат юридичних наук, доцент, полковник Андрій СОРОКА склала цей акт про те, що наукові публікації, наукові положення і

висновки, розроблені за результатами дослідження Вадима ТОРІЧНОГО впроваджено в освітній процес Національної академії Державної прикордонної служби України імені Богдана Хмельницького.

Зокрема, поглиблено змістовно-понятійну базу щодо інформаційного забезпечення державної безпеки, удосконалено механізми інформаційного забезпечення державної безпеки, принципи функціонування державної системи інформаційної безпеки, запропоновано шляхи розвитку єдиної державної політики у сфері інформаційної безпеки в Україні, які знайшли своє відображення в наступних навчальних дисциплінах: «Інформаційна політика та інформаційна безпека», «Наукові основи управління», «Управління повсякденною діяльністю», «Інформаційно-аналітичне забезпечення ОСД», «Інтегроване управління кордонами», «Національна безпека України», «Управління змінами та впровадження інновацій», «Державне управління у сфері національної безпеки».

Результати дисертаційного дослідження також реалізовано в навчально-методичних та довідкових матеріалах для слухачів факультету підготовки керівних кадрів Національної академії Державної прикордонної служби України імені Богдана Хмельницького.

Голова комісії:
професор кафедри прикордонної безпеки,
доктор наук з державного управління, доцент — Геннадій МАГАСЬ

Члени комісії:
головний науковий співробітник науково-дослідного відділу,
доктор наук з державного управління, професор — Валерій ДОВГАНЬ

начальник кафедри національної безпеки
(сфера прикордонної діяльності) та управління,
доктор військових наук, доцент, полковник — Юрій ІВАШКОВ

начальник навчального відділу,
кандидат юридичних наук, доцент, полковник — Андрій СОРОКА