Таким чином, обмін інформацією, координація дій, спільні навчання та операції – це запорука успіху у боротьбі з цими складними та багатогранними загрозами. Лише такий комплексний та системний підхід дозволить зміцнити стійкість інститутів публічної влади та забезпечити стабільне функціонування держави в умовах гібридних загроз.

1. Atkinson, C. (2018). Hybrid warfare and societal resilience implications for democratic governance. *Information & Security*, 39(1), 63-76.
2. Bachmann, S. (2015). Hybrid wars: The 21st-century's new threats to global peace and security. *Scientia Militaria: South African Journal of Military Studies*, 43(1), 77-98.
3. Hoffman, F. (2009). Hybrid threats: Reconceptualizing the evolving character of modern conflict.
4. Johnson, R. (2018). Hybrid war and its countermeasures: a critique of the literature. *Small wars & insurgencies,* 29(1), 141-163.
5. Loza, V., Myronenko, V., Myronenko, P., Smolianiuk, V., & Chelak, O. (2024). The escalation of military threats as a reality of modern geopolitics. *Multidisciplinary Science Journal*, 6, 2024ss0223. URL : https://doi.org/10.31893/multiscience.2024ss0223
6. Missiroli, A. (2024). From hybrid warfare to'cybrid'threats-and back? Concepts, challenges, responses. In Addressing Hybrid Threats (pp. 40-56). Edward Elgar Publishing.

Ірина ВАСНЯТІНА
ад'юнкт кафедри
оперативно-розшукової діяльності
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна)

ДОСЛІДЖЕННЯ ЗНАЧЕННЯ ТА ОСОБЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Інформація – це невід'ємна частина розвитку та життєдіяльності людини. Забезпечення національної безпеки в контексті інформаційної безпеки – це гарант захищеності кожного громадянина країни. Саме законодавство є найбільш ефективним засобом захисту інформаційної безпеки держави та суспільства.

Говорячи про необхідність внесення поточних правок у чинне законодавство з питань інформаційної безпеки, потрібно адекватно оцінювати технологічний аспект, а саме діджиталізацію більшості сфер суспільного життя, що вимагає в недалекій перспективі докорінного перегляду галузевих нормативно-правових актів, які покладені в основу відносин використання баз даних і обміну інформацією [3, с. 35].

В умовах сьогодення для будь-якої держави інформація виступає стратегічно важливим ресурсом, від раціонального використання якого залежить безпека країни та перспективи формування демократичного суспільства, де реалізуються всі конституційні права та свободи громадян [2, с. 64].

Вивченню питання інформаційної безпеки приділяли увагу багато науковців та дослідників, зокрема: П. Біленчук, С. Білько, С. Гнатюк, М. Гончаров, М. Григорчук, О. Дзьобань, О. Довгань, С. Здоровко, О. Золотар, В. Кононенко, О. Косілова, А. Лаутар, В. Ліпкан, О. Логінов, В. Лук'янова, Н. Новицька, В. Петрик, О. Тихомиров, Т. Ткачук, В. Цимбалюк, А. Шевченко, О. Ярема та ін.

Відповідно до п. 3 ч. 1 ст. 1 Закону України «Про інформацію» інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [6].

В свою чергу, у п. 2 ч. 1 ст. 1 Закону України «Про інформацію» вказано, що захист інформації – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [6].

В. Шульга пропонує вибудовувати зміст поняття «інформація» на двох рівнях:

1) макрорівень, коли інформація впевнено займає позиції головного фактора могутності держави, адже здатність держави мати у своєму розпорядженні найсучасніші інформаційні технології дозволяє ефективно управляти інформацією. Володіння державою такою здатністю – шлях до подальшого нарощування своєї політичної та економічної

міцності;

2) мікрорівень, де обсяг, достовірність, цілісність, якість обробки інформації визначає ефективність дій менеджменту підприємства, а отже, актуалізує використання інформаційних технологій в управлінні грошово-кредитними, фінансовими, соціально-економічними процесами даного підприємства [8].

В. Лук'янова та А. Лаутар зазначають, що інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. Під інформаційним середовищем розуміють сферу діяльності учасників інформаційних відносин, пов'язану зі створенням, зміною і споживанням інформації. Дане середовище умовно поділяється на три основні предметні частини: створення і розповсюдження первинної та вторинної інформації; формування інформаційних ресурсів, підготовка інформаційних продуктів, надання інформаційних послуг; споживання інформації та дві забезпечувальні предметні частини: створення і застосування інформаційних систем, інформаційних технологій і засобів їх забезпечення, а також забезпечення недоторканності інформації (інформаційної безпеки) [4, с. 97].

З погляду В. Петрика інформаційна безпека – це стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток, технічний, інтелектуальний, соціально-політичний, морально-етичний, за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди [5, с. 50]. Вважаємо, що В. Петрик найбільш точно визначив поняття інформаційної безпеки.

Отже, зазначимо, що інформаційна безпека є невід'ємною частиною національної безпеки. Стан національної безпеки можна досягти за допомогою правильного тлумачення та використання законодавства, а також функціонування всіх державних установ, які створено для захисту інформації на національному рівні.

Положеннями Закону України «Про національну безпеку України» вводяться поняття воєнної, громадської і державної безпеки, що формують цілісне поняття «національна безпека», котре, у свою чергу, розглядається як узагальнююча категорія в системі провадження заходів із захисту державного суверенітету, цілісності і неподільності території, встановлених конституційних гарантій демократичного вектора розвитку суспільства, а також створення ефективних механізмів нейтралізації джерел загроз українській державності [7].

З вищевикладеного слідує, що законодавство виділяє три види безпеки, а саме:

1) воєнну (захист державних кордонів, суверенітету);

2) громадську (захист конституційних прав, свобод та інтересів людини і громадянина, яких необхідно дотримуватися в демократичному суспільстві);

3) державну (забезпечення механізму захисту національних інтересів).

Українські науковці в процесі дослідження поняття інформаційної безпеки як частини національної безпеки виділили перелік завдань, які необхідно виконати для забезпечення інформаційної безпеки України, а саме:

– забезпечення постійного об'єктивного моніторингу інформаційного простору (внутрішнього та зовнішнього), систематичний аналіз результатів моніторингу;

– чітке визначення єдиного загальнодержавного стратегічного наративу та особливостей його трактування різними державними інституціями України;

– створення механізмів унеможливлення відхилення від наративу при здійсненні інформаційної діяльності різними державними інституціями;

– скоординована діяльність в інформаційному просторі всіх державних інституцій України;

– реалізація принципів та методології стратегічних комунікацій всіма державними інституціями, які здійснюють інформаційну діяльність;

– виявлення, оцінювання та прогнозування наслідків загроз національним інтересам та національній безпеці України в інформаційній сфері;

– протидія зовнішнім інформаційним впливам на населення України, зокрема на воєнно-політичне керівництво, особовий склад всіх складових сектора безпеки і оборони України; захист об'єктів критичної інформаційної інфраструктури України (зокрема від кібератак);

– підвищення медіаграмотності населення [1].

Таким чином, нами у повному обсязі досліджено значення інформації для суспільства та держави, а також встановлено, що інформаційна безпека являє собою

невід'ємну частину національної безпеки, стан якої можна досягти за допомогою виконання окреслених у науковій роботі завдань.

1. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (м. Київ, 26 бер. 2021 р.). Київ : НА СБУ, 2021. 346 с. URL : https://eportfolio.kubg.edu.ua/data/conference/7238/document.pdf.

2. Віннічук О. В. Медіа-віруси як загроза інформаційній безпеці в умовах російсько-української війни. Інформаційна безпека: сучасний стан, проблеми та перспективи : зб. матеріалів Міжнар. наук.-практ. конф. (м. Кам'янець-Подільський, 03 лист. 2022 р.). Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. С. 64–69.

3. Гончаров М. В. Дослідження поняття «інформаційна безпека». *Науковий вісник Ужгородського Національного університету.* 2024. № 1 (82). С. 34–37.

4. Лук'янова В. В., Лаутар А. Ю. Інформаційна безпека в умовах розвитку інформаційної системи. *Вісник Хмельницького національного університету*. 2013. № 2. Т. 3. С. 97–101.

5. Петрик В. М., Галамба М. В. Інформаційна безпека України: поняття, сутність та загрози. *Юридичний журнал*. 2006. № 11. С. 49–52.

6. Про інформацію : Закон України від 02.10.1992. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text.

7. Про національну безпеку України : Закон України від 21 червня 2018 р. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text.

8. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка.* 2015. № 4. URL : http://www.economy.nayka.com.ua/?op=1&z=5514.

Артем ДОРОФЕЄВ
аспірант Національної академії
Служби безпеки України
(м. Київ, Україна)
https://orcid.org/0009-0008-5400-4070

НЕОБХІДНІСТЬ СТВОРЕННЯ СИСТЕМИ СТРАТЕГІЧНОГО СТРИМУВАННЯ ЗАГРОЗ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ УКРАЇНИ

В умовах збройної агресії, яка триває проти України, особливого значення набуває інформаційна складова державної безпеки. Інформаційний простір є не лише середовищем поширення даних, а й важливим інструментом впливу на свідомість та поведінку громадян, формування суспільної думки, а також засобом провокування соціальних і політичних конфліктів. Як наслідок, забезпечення захисту та безпеки інформаційного простору стає одним із пріоритетних завдань держави [1; 2]. З огляду на це постає потреба у формуванні дієвої системи стратегічного стримування, яка б дозволила своєчасно ідентифікувати, оцінювати й нейтралізувати інформаційні загрози. Така система має базуватися на комплексному підході та включати правові, організаційні, технічні, освітні й комунікаційні елементи [3].

В умовах розвитку сучасних інформаційних технологій, загального науково-технічного прогресу держав постають інноваційні загрози, пов'язані з поширенням мілітаризації засобів штучного інтелекту (машинного навчання), квантових технологій, соціальної інженерії та когнітивних операцій тощо, які проводяться у кіберпросторі та/або з його використанням.

Основними інноваційними ризиками та загрозами в інформаційному просторі для забезпечення державної безпеки України слід вважати:

1. Дезінформацію та ворожу пропаганду. Гібридна війна, що ведеться проти України, супроводжується масованою інформаційною кампанією, спрямованою на поширення фейкових новин, маніпулятивних матеріалів, прокремлівських наративів. Дезінформація використовується для нагнітання паніки, підриву довіри до державних інститутів і створення розколу в суспільстві [4];

2. Кібератаки та кіберзагрози. Зростає кількість цілеспрямованих кібератак на державні установи, енергетичний сектор, об'єкти критичної інфраструктури, медіаресурси та інші важливі сфери. Кіберзлочинці та ворожі спецслужби використовують широкий спектр технік – від фішингу до складних програм-шкідників, що призводить до витоку або