УДК 004.056.53
DOI https://doi.org/10.32844/2618-1258.2024.6.14

ШЕВЧУК М.О.

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ: ВИКЛИКИ СЬОГОДЕННЯ

INFORMATION SECURITY OF THE STATE: TODAY'S CHALLENGES

У статті досліджуються актуальні виклики забезпечення інформаційної безпеки держави в умовах розвитку інформаційного суспільства та глобалізації. Акцентується увага на стратегічному аспекті значущості інформації як найціннішого ресурсу сучасного суспільства, що впливає на всі аспекти життєдіяльності держави, від політичної стабільності до економічного розвитку. Особлива увага приділяється загрозам, пов'язаним із деструктивним інформаційним впливом, такими як недостовірна, а подеколи – шкідлива інформація, її несвоєчасне надходження, промислове шпигунство, комп'ютерна злочинність. Також систематизовано теоретико-методологічні погляди науковців до розуміння категорії «інформаційна безпека держави» як важливого показника в контексті забезпечення національної безпеки в умовах глобалізації. Було зазначено, що інформаційний вплив російських медіа під час Євромайдану та подальших подій став одним із ключових чинників втрати інформаційного суверенітету в Криму та на сході України, що створило передумови для анексії та подальших військових дій. Значна увага приділена ролі держави у створенні умов для безпечного функціонування національного інформаційного простору. Особливо акцентується, що інформаційна безпека має забезпечити права та свободи громадян на вільне створення, одержання й розповсюдження інформації. Окрім того, зауважується, що забезпечення інформаційної безпеки є складним і багаторівневим процесом, що вимагає реалізації цільової державної політики. Це включає розробку правових, організаційних, технічних та економічних заходів, а також узгодження національного законодавства із нормами міжнародного права. Зазначено, що ключовими механізмами є прийняття відповідних доктрин, стратегій і програм, спрямованих на зміцнення інформаційної безпеки. У підсумку пропонується визначити інформаційну безпеку як процес захисту національного інформаційного простору, з метою створення умов для його оптимального функціонування та безпечного розвитку міжнародного інформаційного співробітництва. Загалом, стаття наголошує на важливості системного підходу до вирішення проблеми інформаційної безпеки, що охоплює як національний, так і міжнародний рівень.

Ключові слова: *глобалізація, інформаційне суспільство, захист інформації, загрози, безпека, інформаційний простір, інформаційний суверенітет, інформаційні технології, інформаційний вплив, державна політика.*

The article discusses the current challenges of ensuring state information security in the context of the development of the information society and globalization. The author emphasizes the strategic aspect of the importance of information as the most valuable resource in modern society, affecting all aspects of public life, from political stability to economic development. Particular attention is paid to threats to the influence of destructive information, such as unreliable and sometimes harmful information, its timely receipt, industrial espionage, cybercrime. The author also systematizes the theoretical and methodological views of scholars on understanding the category of "information security of the state" as an important indicator in the context of ensuring national security in the context of globalization. It was noted that the information influence of the Russian media during Euromaidan and subsequent events was one of the key factors in

© ШЕВЧУК М.О. – кандидат юридичних наук, докторант кафедри конституційного, адміністративного та фінансового права (Хмельницький університет управління та права імені Леоніда Юзькова)

the loss of information sovereignty in Crimea and eastern Ukraine, which created the preconditions for the annexation and subsequent hostilities. Considerable attention is paid to the role of the state in creating conditions for the safe functioning of the national information space. It is emphasized that information security should ensure the rights and freedoms of citizens to freely create, receive and disseminate information. In addition, it is noted that ensuring information security is a complex and multilevel process that requires the implementation of a targeted state policy. This includes the development of legal, organizational, technical and economic measures, as well as the harmonization of national legislation with international law. It is noted that the key mechanisms are the adoption of appropriate doctrines, strategies and programs aimed at strengthening information security. As a result, the author proposes to define information security as the process of protecting the national information space with a view to creating conditions for its optimal functioning and safe development of international information cooperation. In general, the article emphasizes the importance of a systematic approach to solving the problem of information security, covering both the national and international levels.

Key words: *globalization, information society, information protection, threats, security, information space, information sovereignty, information technology, information influence, public policy.*

Постановка проблеми. Проблематика інформаційної безпеки посідає центральне місце у стратегії державної інформаційної політики сучасної держави. Чому інформаційна безпека така важлива?

− Економічна стабільність: Кібератаки можуть призвести до значних фінансових втрат, порушення роботи критичної інфраструктури та підриву довіри до національної економіки.

− Національна безпека: Захист державної таємниці, протидія дезінформації та пропаганді, забезпечення безпеки виборчих процесів – все це є невід'ємною частиною національної безпеки.

− Соціальна стабільність: Поширення фейкових новин, кібербулінг та інші форми інформаційного насильства можуть підривати соціальну згуртованість та дестабілізувати суспільство.

У короткостроковій, середньостроковій та довгостроковій перспективах прогнозується подальше зростання загроз і викликів у цій сфері на глобальному рівні. Належний захист інформаційних ресурсів є критичним у сфері, оскільки їх недостатня захищеність створює ризик для національної та міжнародної безпеки, а також може призвести до часткової або повної втрати державного інформаційного суверенітету. Розвиток цифрових технологій та зростання взаємозалежності між країнами створюють нові виклики для забезпечення інформаційної безпеки. Серед основних загроз можна виділити:

− Кібератаки: Зловмисні дії, спрямовані на порушення роботи інформаційних систем, крадіжку даних, шантаж та дестабілізацію суспільства.

− Дезінформація та пропаганда: Свідоме поширення неправдивої інформації з метою маніпулювання громадською думкою та підриву довіри до державних інституцій.

− Шпигунство: Незаконне отримання інформації, що становить державну та комерційну таємницю.

− Технологічні ризики: Поява нових технологій, таких як штучний інтелект та квантові обчислення, створює нові можливості для кібератак і вимагає розробки нових засобів захисту.

Для ефективної протидії цим викликам держава повинна керуватися продуманою комплексною стратегією, яка включає скоординовані дії за кращими напрямками, і цілеспрямовано використовувати всі наявні ресурси та засоби.

Аналіз останніх досліджень і публікацій. Дослідження проблематики інформаційної безпеки викладені у працях В. С. Цимбалюка, О. Зернецької, О. Резнікової, М. Галамби, О. В. Олійник, О. Солодкої, В. М. Супрун, В. А. Ліпкан, Л. С. Харченко, О. В. Логінов, Ю. О. Коваленко та ін. Незважаючи на наявні наукові праці, тема інформаційної безпеки залишається актуальною та потребує подальших досліджень, особливо в контексті зростаючих загроз національній безпеці України. Особливого значення має дослідження механізмів запобігання кібератакам, протидії маніпулятивному впливу на свідомість громадян, а також розробка стратегій збереження інформаційного суверенітету. Крім того, важливо забезпечити швидкий розвиток цифрових технологій, які постійно змінюють природу загроз, включаючи штучний інтелект, великі дані та технології

блокчейн, які можуть бути як інструмент захисту, так і новим джерелом ризиків. Тому подальші дослідження повинні зосередитися на адаптації існуючих механізмів до умов цифрової трансформації та інтеграції України до світового інформаційного простору безпеки. Окремої уваги потребує вивчення міжнародного досвіду у сфері інформаційної безпеки.

Мета статті. Метою статті є дослідження актуальних викликів і загроз забезпечення інформаційної безпеки держави в умовах розвитку інформаційного суспільства та глобалізації, аналіз теоретико-методологічних підходів до розуміння категорії «інформаційна безпека» і також обґрунтування значущості забезпечення інформаційної безпеки, вдосконалення процесу забезпечення інформаційної безпеки.

Виклад основного матеріалу. Інформаційне суспільство є одним із типів суспільств, які розвиваються в результаті соціального прогресу. Особливої актуальності інформаційна безпека суспільства набуває в умовах приєднання України до глобальної кіберцивілізації – рівню розвитку інформаційного суспільства, за якого ефективність життєдіяльності його складових визначається досягненнями науково-технічного прогресу: освоєнням комп'ютерних інформаційних технологій як засобів глобальної телекомунікації [1].

Інформаційне суспільство як етап розвитку сучасної цивілізації характеризується збільшенням ролі інформації та знань у житті суспільства, зростанням частки інформаційних продуктів і послуг у валовому внутрішньому продукті, створенням глобального інформаційного простору, який забезпечує ефективну інформаційну взаємодію людей, їхній доступ до світових інформаційних ресурсів і задоволення соціальних та особистісних потреб в інформпродуктах і послугах. Водночас інформаційне суспільство ґрунтується на інформаційних технологіях, «інтелектуальних» комп'ютерах, автоматизації та роботизації всіх сфер і галузей економіки та управління, єдиній сучасній інтегрованій системі зв'язку. Це забезпечує кожній особі доступ до будь-якої інформації і знань та зумовлює радикальні зміни в усій системі суспільних відносин. Інформація є найцінішим глобальним ресурсом, бо економічний потенціал суспільства визначають переважно за обсягом його інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація як така є динамічним феноменом, постійні зміни котрого приводять до трансформації його якості, збільшення кількості інформаційних джерел і споживачів. Відтак, сучасне інформаційне суспільство перебуває під постійною загрозою отримання недостовірної, а подеколи – шкідливої інформації, її несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності тощо [2].

Деструктивний інформаційний вплив (такий як поширення фейкових новин, пропаганди та маніпуляцій) на суспільство може мати негативні наслідки не лише в інформаційній сфері але й економічній, політичній та інших сферах суспільства та держави. Цей вплив часто порівнюють з каскадом, де одна подія спричиняє ланцюгову реакцію, що призводить до серйозних наслідків. На сучасному етапі розвитку інформація – це стратегічний ресурс, що має глобальний вплив. Свідоме нагнітання російськими ЗМІ антиукраїнської істерії під час Євромайдану призвело до втрати Криму через те, що там не знайшлося критичної маси осіб, які чинили б опір «ввічливій окупації», натомість зросла кількість тих, хто схвалював анексію [3]. Свідченням небезпечного характеру цих технологій стало фактичне захоплення росією інформаційного простору Криму, сходу та півдня України, що створило передумови для російської окупації АРК та організації збройного конфлікту в Донецькій і Луганській областях. Російська пропаганда зіграла вирішальну роль у анексії Криму. Вона дозволила росії створити сприятливі умови для проведення незаконного референдуму та подальшої анексії півострова. Цей досвід є важливим уроком для всього світу, який демонструє, наскільки потужною може бути інформаційна зброя. Також це було передумовою початку повномасштабного вторгнення російської федерації на територію незалежної та суверенної України, яке розпочалось 24 лютого 2022 року. Наслідки такої інформаційної війни були руйнівними: підрив довіри до державних інституцій, зростання соціальної напруги та, зрештою, втрата територіальної цілісності держави.

Невід'ємною частиною інформаційного простору, що взаємопов'язаний з інформаційними просторами особи і суспільства є інформаційний простір держави. На сьогодні не можна говорити про ключову роль держави в його формуванні, адже інформація виробляється й циркулює серед великої кількості соціальних агентів – основних суб'єктів «змістового наповнення» інфопростору. Держава відіграє ключову роль у визначенні цілей, пріоритетів і стратегій, а також у формуванні умов і регулювання обігу інформації для її ефективного використання на благо розвитку суспільства. У забезпеченні інформаційної безпеки держави постає складне і важливе завдання, особливо в умовах глобалізації, становлення інформаційного суспільства та інтеграції національного інформаційного простору у світову інформаційну інфраструктуру.

Метою діяльності держави в галузі інформаційної безпеки є створення надійного захисту від інформаційних загроз шляхом розробки та впровадження комплексу правових, організаційних та технічних заходів. Крім цього, інформаційна безпека повинна гарантуватися шляхом проведення цілісної державної програми відповідно до чинного законодавства і норм міжнародного права шляхом реалізації відповідних доктрин, стратегій, концепцій і програм. Можна стверджувати, що інформаційна безпека передбачає можливість безперешкодної реалізації суспільством і окремими його членами своїх конституційних прав, пов'язаних з можливістю вільного одержання, створення й поширення інформації. Для забезпечення належного рівня інформаційної безпеки необхідно застосовувати комплексний підхід, що включає політичні, економічні та організаційні заходи, спрямовані на запобігання, виявлення та нейтралізацію будь-яких загроз, які можуть зашкодити інформаційним правам та інтересам держави і її громадян.

Необхідно зазначити, що поняття «інформаційної безпеки держави» розглядали О. Зернецька, Г. Сащук, О. Резнікова, Г. Почепцов та ін. [4, 5, 6, 7] узагальнено розуміючи, що інформаційна безпека держави – це стан її інформаційної захищеності, за якої спеціальні інформаційні операції, акти зовнішньої інформаційної агресії та негласного зняття інформації (за допомогою спеціальних технічних засобів), інформаційний тероризм і комп'ютерні злочини не завдають суттєвої шкоди національним інтересам [8].

Розглядаючи феномен інформаційної безпеки з точки зору функціонального підходу, О. Олійник [9] визначає її як здійснення комплексу системних превентивних заходів з надання гарантій захисту від негативних інформаційних впливів: життєво важливих інтересів особи, суспільства, держави; політичного, економічного, науково-технологічного, гуманітарного, соціокультурного розвитку, підтримання оборони, державної та екологічної безпеки, системи державного управління на необхідному рівні; забезпечення інформаційного суверенітету та безпечного розвитку національного інформаційного простору; від маніпулювання інформацією, дезінформування та впливів на свідомість, підсвідомість і психіку індивіда, суспільних груп, суспільства в цілому; своєчасність і адекватність заходів протидії та нейтралізації всього спектру негативних безпекогенних чинників, що можуть бути застосовані проти України. Ключовими елементами, що формують систему забезпечення інформаційної безпеки, є інформаційний суверенітет, який визначає ступінь незалежності держави в інформаційній сфері, та національний інформаційний простір, який є середовищем для функціонування та розвитку інформаційних процесів [10].

В.М. Супрун стверджує, що предметну сферу інформаційного суверенітету та інформаційної безпеки доцільно розглядати як єдину, структуровану за предметом дослідження і завданнями предметну сферу, що характеризується спільною терміносистемою. У ролі системо утворюючого чинника виступають інформація (знання) та інформаційні процеси у соціотехнічних системах, які є загальним об'єктом досліджень у предметній сфері інформаційного суверенітету та інформаційної безпеки. Це дало підставу йому констатувати, що категорія «інформаційний суверенітет» є родовим поняттям по відношенню до категорії «інформаційна безпека». Супрун В. М. обґрунтовує, що ці категорії взаємопов'язані та взаємодіють між собою, оскільки реалізація засад інформаційного суверенітету здійснюється за допомогою прийомів та методів інформаційної безпеки [11].

Виходячи з аналізу змісту наведених вище визначень поняття «інформаційної безпеки» можна констатувати, що наразі серед фахівців панує декілька підходів до тлумачення цієї категорії. В першу чергу це «захищеність» основних інтересі держави. Такий підхід сформувався ще коли «безпека» мала конкретне вираження, переважно в речах, і вимірювалася їх станом [12, с. 20]. Тоді інформаційна безпека використовувалась більше в значені «захист інформації»: Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення [13].

Разом з тим, сьогодні, у час активного розвитку інформаційних систем та розширення мережі їх впливу, звуження поняття «безпеки» лише до захисту – це пряме обмеження реалізації її основних функцій: звуження, послаблення, усунення і попередження небезпек та загроз. Раніше загрози розглядалися як зовнішні фактори, які необхідно повністю усунути. Однак, розуміння безпеки еволюціонувало: тепер ми усвідомлюємо, що загрози є невід'ємною частиною будь-якої системи. Тому основний фокус змістився з їхньої ліквідації на управління ризиками, тобто на мінімізацію їхнього негативного впливу на функціонування системи. Наукові дослідження

доводять, що забезпечення інформаційної безпеки – це процес, спрямований на збереження інформаційного суверенітету України та захист її національних інтересів від зовнішніх і внутрішніх загроз [14].

Глобалізація суттєво впливає на парадигму безпеки, зміщуючи фокус з національного рівня на міжнародний. В умовах взаємозалежного світу інформаційна безпека вже не може розглядатися лише через призму національних інтересів. Необхідний комплексний підхід, що враховує як національну інформаційну безпеку, так і міжнародне співробітництво.

Висновки. Отже, з вищевикладеного стає цілком зрозуміло, що забезпечення інформаційної безпеки держави в умовах глобалізації та розвитку інформаційного суспільства є складним і багатогранним завданням, що вимагає комплексного підходу. Аналіз сучасних викликів, таких як дезінформація, маніпуляції свідомістю, кіберзлочинність та інформаційний тероризм, підтверджує необхідність ефективної державної політики, орієнтованої на захист національного інформаційного простору. У цьому контексті важливу роль відіграють не лише правові та технічні інструменти, але й міжнародне співробітництво, спрямоване на формування глобальних механізмів протидії інформаційним загрозам.

Інформаційна безпека держави визначається як процес захисту національного інформаційного простору, спрямований на його стабільне функціонування, безпечний розвиток та інтеграцію в глобальну інформаційну інфраструктуру. Для досягнення цієї мети необхідно запроваджувати системний підхід, який охоплює правові, технічні, організаційні та міжнародні заходи, спрямовані на ефективне протистояння загрозам та забезпечення стійкості інформаційної системи держави. Таким чином, зміцнення інформаційної безпеки є основою для збереження сталого розвитку держави, її суверенітету та забезпечення соціальної стабільності в умовах сучасних глобальних викликів.

Підсумовуючи напрацювання відносно національної інформаційної безпеки можемо сформулювати власне визначення інформаційної безпеки держави. Інформаційна безпека держави – це процес захисту національного інформаційного простору з метою створення умов для його оптимального функціонування та безпечного розвитку міжнародного інформаційного співробітництва.

Список використаних джерел:

1. Цимбалюк В.С. Сутність інформаційної безпеки в умовах входження України до глобальної кіберцивілізації. *Науковий вісник академії ДПС України*. 2007. № 4. С. 174–178.

2. Про захист суспільної моралі: Закон України від 20 листопада 2003 року. К.: Парлам. видво, 2003. (Серія «Закони України»).

3. Телелим В. М. Теорія військового мистецтва. *Наука і оборона*. 2014. № 3. С. 38.

4. Зернецька О. Інформаційна безпека в інформаційному суспільстві: глобалізаційні загрози та ризики. *Інформаційне суспільство: Антологія*. К.: ІМВ,2006. С.315−323.

5. Сащук Г.М. Безпекові виміри телепростору: Монографія. К.: Грамота, 2007. С.16.

6. Резнікова О. Оновлення Стратегії національної безпеки України у контексті нових викликів і загроз. *Віче*. 2015. № 5. С.12−22.

7. Почепцов Г. Перші дослідження в галузі інформаційних війн: від минулого до сучасності. URL: http://osvita.mediasapiens.ua/trends (дата звернення 19.01.2025)

8. Галамба М. Інформаційна безпека України: поняття, сутність та загрози. *Юридичний журнал*. 2006. № 11. С.11−18.

9. Олійник О.В. Інформаційний суверенітет як важлива умова забезпечення інформаційної безпеки України. *Наукові записки Інституту законодавства Верховної Ради України*. 2015. № 1. С. 54-59.

10. Солодка О. Інформаційний суверенітет та інформаційна безпека України: діалектика понять. *Evropský politický a právní diskurz*. 2020. С. 233–239.

11. Супрун В. М. Теоретико-правові основи інформаційного суверенітету: автореф. дис. … канд. юрид. наук: спец. 12.00.01 – «теорія та історія держави і права; історія політичних і правових учень». Х., 2010. 20 с.

12. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. К.: КНТ, 2006. 280 с.

13. Коваленко, Ю. О. (2010). Забезпечення інформаційної безпеки на підприємстві. *Економіка промисловості*. № 3. с. 123–129.

14. Ліпкан В. А. Інформаційна безпека України : глосарій / В. А. Ліпкан, Л. С. Харченко, О. В. Логінов . Київ : Текст, 2004. 136 с.