ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 351:329
DOI https://doi.org/10.32782/TNU-2663-6468/2024.4/24

Кучменко В.О.
Державний університет «Житомирська політехніка»

Єнічев М.І.
Державний університет «Житомирська політехніка»

МІСЦЕ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ВАЖЛИВОЇ СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У статті аналізується роль інформації у забезпеченні національної безпеки у сучасному високотехнологічному світі. Вона є фундаментом для прийняття обґрунтованих рішень, які спрямовані на захист національних інтересів та нейтралізацію реальних та потенційних загроз. Інформація забезпечує державним органам можливість адекватно оцінювати поточну ситуацію країни, прогнозувати майбутні виклики та планувати ефективні стратегії реагування на можливі та реальні загрози. В епоху глобалізації, інформаційно-технологічного прориву та посилення взаємозалежності держав, роль інформації стає ще більш важливою, оскільки вона дозволяє не лише адаптуватися до швидкозмінних умов, але й активно формувати безпековий порядок денний. У цьому контексті, аналіз значення інформації для національної безпеки є актуальним і необхідним для розуміння сучасних викликів та можливостей у сфері державного управління.

Оскільки в сучасному світі інформація стала одним з найцінніших ресурсів, впливаючи на всі аспекти життя суспільства, економіки та державного управління, формування інформаційної безпеки є ключовим завданням для будь-якої держави, адже забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів прямо впливає на національну безпеку. Особливість цього процесу полягає в комплексному підході, що поєднує технічні, організаційні, правові та психологічні аспекти захисту. Важливо розуміти, що інформаційна безпека охоплює не лише захист від кіберзагроз, але й створення надійної інфраструктури, яка може протистояти як внутрішнім, так і зовнішнім загрозам. Враховуючи усі події, які відбуваються на території нашої країни, питання забезпечення інформаційної безпеки як невід'ємної та важливої складової національної безпеки стоять особливо гостро. Така значимість пояснюється загостренням таких проблем, як: необхідність захисту суспільства від внутрішніх та зовнішніх інформаційних загроз; прагнення створення сприятливих умов для подальшого розвитку українського суспільства та держави в цілому; загострення економічної кризи; порушення прав і свобод людини і громадянина не лише в Україні, а й також за її межами; підвищення рівня злочинності та корумпованості; загострення демографічної кризи.

Ключові слова: *інформація, безпека, інформаційна безпека, національна безпека, держава, державна безпека.*

Постановка проблеми. У сучасному світі, де цифрові технології стали невід'ємною частиною повсякденного життя, інформаційна безпека набула надзвичайної актуальності. Різке зростання обсягів інформації, яка передається та зберігається в електронному вигляді, поряд з постійним розвитком кіберзагроз, висуває нові вимоги до захисту даних. Інформаційна безпека стала ключовим елементом національної безпеки, оскільки будь-яка вразливість у цій сфері може призвести до серйозних наслідків для держави, економіки та суспільства. Забезпечення надійного захисту інформації є критичним для збереження суверенітету, стабільності та процвітання країни в умовах глобалізації та цифрової трансформації. Інформаційна безпека відіграє виняткову роль у загальній системі національної безпеки держави, оскільки є інтегрованою у всі її скла-

дові, надаючи при цьому самостійного значення. Будь-які виклики чи загрози національній безпеці країни безпосередньо впливають на її інформаційний аспект. Сучасна українська соціально-економічна ситуація, а також недоліки в організації державної влади та громадянського суспільства породжують значний спектр внутрішніх загроз для інформаційної безпеки країни. Зважаючи на вищезазначене виникає необхідність підвищення рівня інформаційної безпеки як складової національної безпеки.

Аналіз останніх досліджень і публікацій. Вивченням ролі інформаційної безпеки як складової національної безпеки були присвячені праці таких вітчизняних вчених як: Арістова І. [1], Бондар І. [2], Дикий А. [4], Дика О. [4], Наумчук К. [4], Супрун В. [8], Тростенюк Т. [4] та інші. В своїх працях дослідники акцентують увагу та важливості інформаційної безпеки втім не достатньою увагу приділяють загрозам, які виникають.

Постановка завдання. Метою статті є визначення ролі інформаційної безпеки як важливої складової національної безпеки.

Викладення основного матеріалу. Швидкий розвиток інформаційних технологій, повсюдна комп'ютеризація та створення глобального інформаційного простору сприяли формуванню інформаційного суспільства, яке нині володіє величезним потенціалом і має вирішальний вплив на розвиток держави та її інноваційні можливості. Незважаючи на еволюційну необхідність створення інформаційного суспільства, його розвиток призвів до виникнення численних загроз у ключових галузях народного господарства, в тому числі й загроз сфери національної безпеки. Повномасштабне вторгнення, на превеликий жаль, змусило кожного з нас відчути не лише збройну агресію, але й інформаційну, яка активно поширювалась та продовжує ширитись через різноманітні засоби масової інформації.

Саме тому, питання національної безпеки набуває особливої важливості в умовах війни, коли країна опиняється під загрозою з боку зовнішніх агресорів, які мають психологічний вплив ще й в середині самої країни. Ситуація в Україні наочно демонструє, наскільки критичною є необхідність своєчасно використовувати здатність держави забезпечувати захист своїх громадян, територіальної цілісності та суверенітету. Війна підкреслила необхідність комплексного підходу до національної безпеки, що включає військову, політичну, економічну, інформаційну та екологічну складові. В цих умовах важливо не лише протистояти безпосередній військовій агресії, але й забезпечувати стабільність усіх сфер державного життя, щоб зберегти стійкість суспільства та його здатність до саморозвитку.

Повномасштабне вторгнення росії на територію України загострило питання захисту національного інформаційного простору, висунувши його на перший план. Необхідність негайного реагування на цю проблему обумовлена інформаційною загрозою державній безпеці України. Відомо, що через інформаційний вплив іншої сторони на свідомість, підсвідомість, інформаційні ресурси та інші об'єкти інформаційної інфраструктури країни можна нав'язати особистості, суспільству чи державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної та державної діяльності, керуючи їхньою поведінкою та розвитком у потрібному напрямку. Це становить загрозу суверенітету України у ключових галузях народного господарства на інформаційному рівні [6].

Вперше за часи незалежності кожен з нас зіштовхнувся з достатньо потужнім інформаційним впливом, що значно погіршувало психоемоційний стан, який і так був достатньо складним. Що ж являє собою інформаційний вплив – це процес, через який інформаційні ресурси, медіа, комунікаційні канали або технології використовуються для зміни думок, переконань, поведінки або рішень окремих осіб, груп чи суспільств в цілому.

Інформаційний вплив може суттєво змінювати стан інформаційної безпеки як в позитивну, так і негативну сторони. Основні аспекти цього впливу, які ми можемо відчути в повсякденному житті це:

– Загроза дезінформації та фейкових новин. До них можемо віднести розподіл неправдивої інформації. Фейкові новини та дезінформація можуть дезорієнтувати громадськість, викликати паніку, створювати хибне уявлення про реальні події. Це підриває довіру до офіційних джерел інформації та створює плутанину; зниження довіри до інформаційних систем. Систематичне поширення неправдивих відомостей може підірвати довіру до медіа та інших джерел інформації, що негативно вплине на здатність громадян і організацій адекватно реагувати на реальні загрози.

– Маніпуляція громадською думкою. Цей процес характеризується формуванням хибних уявлень. Використання інформації для маніпуляцій може змусити людей приймати рішення на основі викривлених або неповних даних. Це може призвести до соціальних і політичних криз, підривати

стабільність суспільства; сприяння конфліктам. Інформаційні кампанії, спрямовані на розподіл або підсилення конфліктів, можуть посилити соціальну напруженість і загрожувати внутрішній безпеці.

– Кібернапади та інформаційні атаки. Різного роду хакерські атаки. Атаки на інформаційні системи можуть порушити конфіденційність, цілісність та доступність даних, що загрожує національній безпеці; шантаж та крадіжка даних: Отримані в результаті атак дані можуть бути використані для шантажу, маніпуляції або як інструмент для подальших атак.

– Соціальна інженерія. Досить загрозливе явище, адже характеризується отриманням конфіденційної інформації. Методи соціальної інженерії використовуються для обману людей з метою отримання чутливих даних, що може призвести до витоку інформації та загрози безпеці; зміна поведінки користувачів. Спрямовані атаки на психічний стан або довіру користувачів можуть призвести до небезпечних дій або необережного поводження з інформацією.

– Політична дезінформація. Вплив на вибори та політичні процеси. Спроба вплинути на результати виборів або політичні рішення через маніпуляцію інформацією може дестабілізувати державні інститути та процеси; посилення політичних розбіжностей. Інформаційні кампанії, спрямовані на розподіл або підсилення політичних розбіжностей, можуть завадити національному єдності та стійкості.

Отже, враховуючи вищевикладену інформацію важливо зазначити, що сучасний стан управління інформаційною безпекою значною мірою відстає від темпів розвитку сучасної інформатизації, що сприяє зростанню рівня кіберзлочинності. Таким чином, всі дії з боку країни агресора спрямовані на поширення загроз які, у свою чергу, можуть призводити до серйозних, а іноді і незворотних наслідків для держави, підприємств, суспільства та окремих осіб. Якщо розглядати ситуацію у глобальному масштабі, існує широкий спектр кіберзлочинів, включаючи ті, що спрямовані на отримання фінансової вигоди, пов'язані з використанням інформації з комп'ютерів, планшетів та мобільних телефонів, а також злочини, які загрожують конфіденційності, цілісності та доступності комп'ютерних систем. Саме тому нам варто зазначити наслідки які можуть виникнути в результаті бездіяльності держави в разі існування негативного інформаційного впливу та активного формування інформаційних загроз:

Економічні наслідки – група наслідків які є одними з найзначніших аспектів негативного інформаційного впливу. Численні кібератаки та інформаційні кампанії можуть завдати значної фінансової шкоди, включаючи прямі збитки через крадіжки даних і витрати на відновлення інформаційних систем, також відбувається порушення різноманітних бізнес-процесів через атаки на корпоративні системи, що призводить до затримок у виконанні контрактів, зниження продуктивності та навіть до банкрутства компаній. В результаті цього може постраждати національна економіка, оскільки вона повною мірою залежить від стабільності і ефективності бізнесу.

Політичні наслідки – група наслідків, які мають прямий негативний інформаційний вплив, оскільки можуть дестабілізувати внутрішню ситуацію в країні. Інформаційні кампанії, що активно маніпулюють громадською думкою, можуть спричинити різного роду соціальні протести, зміни в політичному ландшафті або навіть призвести до революційних змін у владі. Втрата міжнародної репутації через негативну інформацію може ускладнити дипломатичні відносини та знизити ефективність зовнішньої політики держави.

Соціальні наслідки – група наслідків, які більшою мірою зосереджуються на соціально вразливих групах населення. Дезінформація та маніпуляції серед людей може посилити соціальні конфлікти, розділити суспільство на ворожі групи та підвищити рівень насильства. Психологічний вплив негативної інформації може викликати паніку та стрес серед населення, що негативно вплине на загальний соціальний клімат.

Безпекові наслідки – група наслідків, яка не залишає осторонь і критично важливі інфраструктури. Атаки на енергетичні мережі, транспортні системи та комунікаційні канали можуть паралізувати важливі функції держави і призвести до катастрофічних наслідків. Крім того, підвищений ризик тероризму і шпигунства може виникнути внаслідок проникнення в інформаційні системи, що загрожує суверенітету держави.

Правові наслідки – група наслідків яка включає порушення прав і свобод кожного громадянина. Зазвичай проявляється як втручання в приватність і несанкціонований доступ до особистих даних. Негативні інформаційні кампанії можуть також спричинити юридичні конфлікти як на внутрішньому, так і на міжнародному рівнях.

Інноваційні наслідки – група наслідків яка прослідковується через існування ненадійного захисту інформаційних систем та може стриму-

вати інвестиції в нові технології та інновації, що уповільнить економічний розвиток та знизить конкурентоспроможність країни на міжнародній арені.

Саме тому, досить важливо усвідомлювати, що поширення негативного інформаційного впливу та підрив інформаційної безпеки можуть мати далекосяжні наслідки для національної безпеки.

Висновки. Підсумовуючи вищевикладений матеріал слід зауважити, що інформаційна безпека є невід'ємною частиною національної безпеки яка безпосередньо впливає на кожну її складову оскільки без інформації та інформаційного обміну не можливо уявити існування високорозвиненої країни.

Актуальність місця та значення інформаційної безпеки як важливої складової національної безпеки відображається через значну кількість не лише потенційних але й реальних загроз які ми можемо щоденно спостерігати через різноманітні засоби поширення інформації. Оскільки усі суспільні інститути значною мірою залежать від інформаційного простору, вони є частиною інформаційного простору держави, тому негативний інформаційний вплив безпосередньо впливає на їх роботу. Взаємодія держави та громадян є запорукою демократії, а отже – групи загроз які виникають можуть підривати недовіру громадян до апарату державного управління. Враховуючи різноманітні кібератаки та інформаційні впливи інформаційна політика країни повинна враховувати усі загрози при забезпеченні національної безпеки адже якісне інформаційне забезпечення буде невід'ємною частиною задоволення інформаційних потреб національної безпеки.

Слід пам'ятати, що в сучасному світі інформація є не лише ресурсом, але й критично важливим компонентом кожної сфери діяльності країни, якісна і захищена інформація впливає на можливість адекватно оцінювати усі можливості та загрози, що впливають на підтримку життєдіяльності країни, її суверенності та незалежності.

Список літератури:

1. Арістова І.В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія. Х. : Нац. ун-т внутр. справ, 2006. 354 с

2. Боднар І.Р. Інформаційна безпека як основа національної безпеки. Mechanism of Economic Regulation. 2014. № 1. С. 68–75.

3. Гуцалюк М. Інформаційна безпека в сучасному суспільстві. *Право України.* 2005. № 7. С. 71–74.

4. Дикий А.П., Дика О.С., Наумчук К.М., Тростенюк Т.М. Понятійно-категоріальний апарат інформаційної безпеки України в забезпеченні національної безпеки. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування*. 2022. № (4). С. 23–31.

5. Домбровська С.М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. *Теорія та практика державного управління.* 2015. Вип. 1. С. 203–207.

6. Панченко О. Інформаційна безпека держави як елемент соціокультури. *Аспекти публічного управління*. 2020. № 1. С. 58–67.

7. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

8. Супрун В. М. Інформаційний суверенітет як один з елементів інформаційної безпеки держави: теоретико-правовий аспект. *Вісник Харківського національного університету ім. В.Н. Каразіна. Серія: Право.* 2009. № 841. С. 136–139.

Kuchmenko V.O., Yenichev M.I. THE PLACE OF INFORMATION SECURITY AS AN IMPORTANT COMPONENT OF NATIONAL SECURITY

In today's high-tech world, information plays a crucial role in ensuring national security. It is the foundation for making informed decisions aimed at protecting national interests and neutralizing real and potential threats. Information provides state bodies with the opportunity to adequately assess the country's current situation, predict future challenges, and plan effective response strategies to possible and real threats. In the era of globalization, information technology breakthrough and increasing interdependence of states, the role of information becomes even more important, as it allows not only to adapt to rapidly changing conditions, but also to actively shape the security agenda. In this context, the analysis of the importance of information for national security is relevant and necessary for understanding modern challenges and opportunities in the field of public administration.

Since in the modern world information has become one of the most valuable resources, affecting all aspects of society, economy and state administration, the formation of information security is a key task for any state, because ensuring the integrity, confidentiality and availability of information resources directly affects national security. The peculiarity of this process is a comprehensive approach that combines technical, organizational,

legal and psychological aspects of protection. It is important to understand that information security covers not only protection against cyber threats, but also the creation of a reliable infrastructure that can withstand both internal and external threats. Taking into account all the events taking place on the territory of our country, the issue of ensuring information security as an integral and important component of national security is particularly acute. Such importance is explained by the aggravation of such problems as: the need to protect society from internal and external informational threats; striving to create favorable conditions for the further development of Ukrainian society and the state as a whole; aggravation of the economic crisis; violation of human and citizen rights and freedoms not only in Ukraine, but also abroad; increase in the level of crime and corruption; aggravation of the demographic crisis.

Key words: *information, security, information security, national security, state, state security.*