УДК 329.09.5
DOI https://doi.org/10.32782/2408-9257-2023-6-25

Шевчук М. О.,
кандидат юридичних наук,
докторант кафедри конституційного, адміністративного та фінансового права
Хмельницького університету управління та права імені Леоніда Юзькова

АКТУАЛІЗАЦІЯ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ

UPDATING THE ISSUE OF INFORMATION SECURITY IN MODERN CONDITIONS

Стаття висвітлює актуальність та важливість інформаційної безпеки у сучасному інформаційному суспільстві, де швидкий розвиток технологій та зміна соціальних взаємодій створюють нові виклики та загрози. Зміни у соціальних взаємодіях та нормах підсилюють почуття невизначеності та психологічного дискомфорту, роблячи суспільство вразливим до інформаційних загроз. В статті акцентується на критичній ролі оборони інформаційної безпеки, як зазначено в Конституції України, та на законодавчому визначенні інформаційної безпеки, що охоплює захист життєво важливих інтересів суспільства та держави.

Стаття розкриває, що інформаційна безпека є складною структурою, що включає захист від різноманітних внутрішніх та зовнішніх загроз, та залежить від багатьох факторів, включаючи глобальну політичну ситуацію та розвиток інформаційно-технологічного сектору. Державне управління інформаційною безпекою визначається як ключовий елемент забезпечення стабільності та процвітання держави, вимагаючи розробки та імплементації комплексних стратегій захисту інформаційного простору.

Автори підкреслюють, що основні цілі національної інформаційної політики повинні бути спрямовані на захист інформаційного суверенітету та забезпечення доступу до достовірної інформації. Важлива роль приватного сектору та необхідність ефективної організаційно-правової бази для реалізації інформаційної безпеки також обговорюються.

Стаття вказує на важливість протидії інформаційним загрозам, включаючи кібератаки, дезінформацію, та кіберзлочинність, у контексті глобальних інформаційних війн, а також на необхідність підвищення медіакультури та обізнаності громадян. Викладені стратегічні напрямки державного управління інформаційною безпекою включають підвищення медіаграмотності, розвиток системи стратегічних комунікацій та протидію дезінформації, з метою забезпечення комплексного підходу до захисту інформаційного простору та національних інтересів.

Ключові слова: *державне управління, інформаційна безпека, кіберзагрози, стратегічні комункації, протидія дезінформації, медіаграмотність.*

The article highlights the relevance and importance of information security in the modern information society, where the rapid development of technologies and changes in social interactions create new challenges and threats. Changes in social interactions and norms increase feelings of uncertainty and psychological discomfort, making society vulnerable to informational threats. The article focuses on the critical role of defense of information security, as stated in the Constitution of Ukraine, and on the legislative definition of information security, which covers the protection of vital interests of society and the state.

The article reveals that information security is a complex structure that includes protection against various internal and external threats and depends on many factors, including the global political situation and the development of the information technology sector. State management of information security is defined as a key element of ensuring the stability and prosperity of the state, requiring the development and implementation of comprehensive strategies for the protection of the information space.

The authors emphasize that the main goals of the national information policy should be aimed at protecting information sovereignty and ensuring access to reliable information. The important role of the private sector and the need for an effective organizational and legal framework for the implementation of information security are also discussed.

The article points to the importance of countering information threats, including cyberattacks, disinformation, and cybercrime, in the context of global information wars, as well as the need to increase media culture and citizen awareness. The stated strategic directions of state management of information security include increasing media literacy, developing a strategic communications system, and countering disinformation, with the aim of ensuring a comprehensive approach to the protection of information space and national interests.

Key words: *public administration, information security, cyber threats, strategic communications, countering disinformation, media literacy.*

Постановка проблеми. В контексті збільшення інформаційних викликів, особливо після введення воєнного стану в Україні указом Президента 24 лютого 2022 року [1], виникає гостра потреба у формуванні комплексної державної політики в сфері інформаційної безпеки. Це включає розробку стратегій та практичних механізмів, спрямованих на протидію інформаційно-психологічному впливу, інформаційній експансії та інформаційним війнам воєнного часу.

Стан опрацювання. Тема інформаційної безпеки займає значне місце в наукових дослідженнях багатьох вчених, серед яких М. Гаврильців, О. Косогов, А. Сірик та інші. Їх роботи охоплюють широкий спектр питань, від правового регулювання до конкретних аспектів забезпечення безпеки в інформаційному просторі. Дослідники як в Україні, так і за кордоном активно вносять вклад у розвиток цієї галузі, розробляючи теоретичні основи та практичні рекомендації для зміцнення інформаційної безпеки.

Метою статті є комплексний аналіз і систематизація наявних наукових поглядів на забезпечення інформаційної безпеки в Україні, а також розробка рекомендацій щодо вдосконалення державного управління в цій сфері на основі вивчення вітчизняного та міжнародного досвіду.

Виклад основного матеріалу дослідження. У сучасному світі, який стрімко розвивається завдяки поступу в галузі інформаційних та комунікаційних технологій, інформаційна безпека стає одним з ключових пріоритетів для забезпечення стабільності та благополуччя суспільства. Розвиток інформаційного суспільства, заснованого на використанні різноманітної інформації, призвів до змін у соціальних взаємодіях, нормах та правилах, викликаючи у людей почуття дезорієнтації та невизначеності у своєму місці в суспільстві. Ця динаміка створює підґрунтя для зростання соціальної незахищеності та психологічного дискомфорту, роблячи людину вразливою до інформаційних загроз.

Конституція України підкреслює критичну роль оборони інформаційної безпеки країни, акцентуючи на необхідності охорони суверенітету, територіальної неділимості, економічного благополуччя та інформаційного простору як ключових завдань уряду, що є відповідальністю усього народу (ст. 17) [2].

Законодавче визначення інформаційної безпеки зафіксоване в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.»: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» (п. 13 Закону) [3].

Інформаційна безпека представляє собою складну структуру з різними рівнями, що взаємодіють, яку формують як внутрішні, так і зовнішні впливи. Серед ключових факторів, що впливають на неї, можна виділити глобальну політичну ситуацію, потенційні загрози безпеці, ступінь розвитку інформаційно-технологічного сектору в країні, та політичну стабільність в межах держави. Ця система включає в себе захист індивідуальних, державних та суспільних інтересів, спрямований на підтримку стабільного і прогресивного розвитку [4, с. 154–155].

Держава, визнаючи значення інформаційної безпеки, приймає на себе відповідальність за розробку та імплементацію комплексних стратегій, спрямованих на захист інформаційного простору від внутрішніх та зовнішніх загроз. Це включає не лише захист від кібератак і дезінформації, але й забезпечення права громадян на доступ до достовірної інформації, особливо в умовах воєнної агресії та інформаційно-психологічних операцій. Таким чином, державне управління інформаційною безпекою стає вирішальним фактором у забезпеченні стабільності та процвітання держави.

Основні цілі інформаційної політики країни повинні бути спрямовані на захист інформаційного суверенітету, забезпечення національного інформаційного простору, і реалізацію конституційних прав громадян на доступ до інформації. Це вимагає створення ефективної організаційно-правової бази, яка б включала в себе чітко визначені органи влади, задіяні у формуванні та реалізації інформаційної безпеки, а також систему правових норм, що регулюють цю сферу.

Як слушно зазначає М. Гаврильців, забезпечення інформаційної безпеки завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії значною мірою може сприяти забезпеченню досягнення успіху при вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Так, втілення в життя вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних і військових конфліктів [5, с. 201].

Важливо також зазначити роль приватного сектору, включаючи виробничі підприємства та інші суб'єкти господарювання, у забезпеченні інформаційної безпеки. Сучасні інформаційні системи, які використовуються підприємствами для автоматизації своєї діяльності, повинні бути належно захищені від різних загроз, щоб забезпечити цілісність, конфіденційність та доступність інформації, що зберігається.

Основні фактори, що негативно впливають на інформаційний простір України, включають втрати в особовому складі, недосконаліть системи інформаційної безпеки, що підриває довіру до політичного та військового керівництва, та активність інформаційної агресії з боку росії, яка формує уявлення про федералізацію як прийнятний шлях для України [6, с. 39].

Стратегія національної безпеки України визначає інформаційну війну та відсутність цілісної комунікаційної політики як ключові загрози, що вимагають підвищення медіакультурності громадян для протидії. Значну увагу потребує також кібербезпека, оскільки кіберпростір використовується для широкого спектру підривних дій [7, с. 18].

Актуальність інформаційної безпеки в сучасних умовах полягає у необхідності захисту суспільства від дезінформації, шпигунства та кіберзлочинності, що є елементами гібридної війни, спрямованими на підрив національної свідомості та державної цілісності.

У контексті російсько-українського конфлікту, кіберактивність значно виходить за рамки дій державних структур. Зауважено, що недержавні кібератори, представники обох сторін конфлікту, зосередили свої атаки на широкий спектр цілей, включаючи фінансовий сектор, використовуючи такі методи, як розподілені атаки на відмову в обслуговуванні (DDoS). Це підкреслює вразливість секторів, які традиційно не асоціюються з кібервійною.

Одним з прикладів є дії проросійської хакерської групи NoName057, яка погрожувала атакувати фінансовий сектор України, що призвело до серії DDoS-атак на українські банки протягом декількох днів. Такі дії не лише спричиняють безпосередню шкоду враженим організаціям, але й викликають значні збої в економіці та підривають довіру до фінансової інституцій країни. Це також спонукає до вдосконалення заходів безпеки та розробки нових стратегій захисту.

Окрім фінансового сектору, значна увага кіберзлочинців прикута до українських державних структур. Наприклад, атака на український онлайн-сервіс «єЧерга», що використовується для бронювання місць для перетину кордону вантажівками, виявила стратегічну ціль кібератак – паралізувати критично важливі державні сервіси та викликати соціальний та економічний дисбаланс.

Росія також використовує кібератаки для спроб зламу акаунтів у месенджері SIGNAL, що є популярним засобом комунікації серед українських військовослужбовців та вважається захищеним від зовнішніх втручань. Це демонструє намір атакувати не лише інфраструктурні об'єкти, але й персональні дані та приватну комунікацію.

Згідно з даними Держспецзв'язку, протягом першої половини 2023 року кількість кібератак проти України значно зросла, хоча кількість критичних нападів знизилась, що може свідчити про зміцнення захисту інформаційних систем. Така динаміка вказує на необхідність постійного аналізу кіберзагроз та адаптації захисних механізмів до змінюваних тактик та стратегій кіберзлочинців.

В умовах глобальної кібервійни, інформаційна безпека вимагає комплексного підходу, що включає міжнародну співпрацю, розробку передових технологій захисту, а також підвищення обізнаності громадян та організацій щодо потенційних кіберзагроз і методів їх протидії.

Аналіз сучасних викликів і загроз інформаційній безпеці висвітлює важливість розуміння та протидії кіберзагрозам, які невпинно розвиваються в епоху цифровізації. Розвиток вели-

ких мовних моделей, таких як GPT-4, Claude, і PaLM2, відкриває нові горизонти для технологічного прогресу, але разом з тим створює потенціал для зловмисного використання. Інструменти, здатні генерувати переконливий текст, можуть бути використані для створення фішингових кампаній або для розповсюдження дезінформації.

Кіберзлочинці можуть використовувати ці технології для створення шкідливого коду, глибоких фейкових відео або для здійснення атак соціальної інженерії. Наприклад, генерація голосових повідомлень штучним інтелектом є значним ризиком для психологічного впливу та маніпулювання, особливо в контексті соціальної інженерії, де може бути використано для імітації голосів відомих осіб або для створення переконливих шахрайських повідомлень.

Сучасні рішення для керованої передачі файлів (Managed File Transfer, MFT) відіграють ключову роль у безпечному обміні конфіденційними даними в бізнес-операціях. Однак, вони також можуть стати ціллю для кіберзлочинців через величезну кількість зберіганої конфіденційної інформації, включаючи інтелектуальну власність та особисті дані.

Програмне забезпечення-вимагач, яке поширюється через шкідливі вкладення електронної пошти або веб-сайти, продовжує залишатися серйозною загрозою для інформаційної безпеки. Групи, які використовують програмне забезпечення-вимагач, такі як CLOP, експлуатують вразливості в системах, таких як Accellion FTA, викликаючи втрату конфіденційних даних та серйозні порушення в роботі організацій.

Міжнародні відносини також мають прямий вплив на інформаційну безпеку. Кіберпростір стає ареною для міждержавних конфліктів, де країни використовують кібероперації для досягнення своїх геополітичних цілей, що підвищує ризики для національної безпеки.

У відповідь на ці загрози, держави та організації повинні розробляти та впроваджувати комплексні стратегії інформаційної безпеки, які охоплюють як технічні заходи, так і стратегії протидії соціальній інженерії, а також забезпечують відповідальне використання та контроль за штучним інтелектом і іншими технологіями.

У контексті практичних аспектів забезпечення інформаційної безпеки в Україні, стратегія інформаційної безпеки до 2025 року [9] передбачає низку ключових напрямів. Серед них важливе місце займає підвищення рівня медіакультури та медіаграмотності, забезпечення дотримання конституційних прав особи, в тому числі свободи вираження та протидія поширенню незаконного контенту. Особливу увагу приділяється розвитку ефективної системи стратегічних комунікацій та протидії дезінформації, що включає створення механізмів раннього виявлення загроз та взаємодії у сфері інформаційної політики між різними органами державної влади та громадськими інституціями.

Кабінет Міністрів України також схвалив цю Стратегію, наголошуючи на її ролі у захисті національної інформаційної безпеки та встановленні чіткого розподілу обов'язків між органами влади для ефективної реалізації стратегічних цілей. Важливою складовою є розвиток законодавства, що регулює відповідальність за поширення дезінформації та обмеження доступу до шкідливого контенту в українському сегменті Інтернету, забезпечення відповідності цих заходів міжнародним стандартам і практиці ЄСПЛ, уникнення надмірного втручання держави у визначення правдивості інформації.

Роль освіти та підвищення обізнаності в контексті зміцнення інформаційної безпеки не може бути недооціненою. Важливим є проведення цілеспрямованої психолого-просвітницької роботи, особливо у сферах, які потенційно можуть стати мішенями інформаційних атак, таких як військові частини або військовослужбовці. Забезпечення технічної безпеки інформаційних систем, що використовуються у військах, також є критично важливим для запобігання умисному пошкодженню систем або крадіжці конфіденційної інформації.

На нашу думку, можна виділити декілька ключових аспектів, які відіграють важливу роль у формуванні ефективної стратегії державного управління інформаційною безпекою. Серед них:

1. Підвищення рівня медіакультури та медіаграмотності є важливими компонентами стратегії інформаційної безпеки, що дозволяють громадянам критично оцінювати інформацію та протидіяти дезінформації.

2. Розробка та впровадження системи стратегічних комунікацій допомагають координувати зусилля різних органів державної влади та громадських інституцій у сфері інформаційної безпеки, забезпечуючи єдину та послідовну політику.

3. Протидія дезінформації. Стратегія передбачає розробку механізмів раннього виявлення інформаційних загроз та протидію дезінформації, що включає вдосконалення законодавства та співпрацю з громадськими інституціями.

Ефективність заходів інформаційної безпеки залежить від комплексного підходу, який включає якісний доступ до інформації, свободу вибору джерел та захист від шкідливого впливу інформації. Важливим завданням є розробка заходів для нейтралізації інформаційної агресії та запобігання її поширенню, що допоможе зберегти національні інтерес.

Висновки. Державне управління інформаційною безпекою передбачає розробку та реалізацію комплексних стратегій, спрямованих на захист від внутрішніх та зовнішніх загроз, включаючи кібератаки, дезінформацію та інші форми інформаційної агресії. Важливу роль у цьому процесі відіграє забезпечення права громадян на доступ до достовірної інформації, особливо в критичних ситуаціях.

Стратегічні напрямки державного управління мають бути спрямовані на зміцнення інформаційного суверенітету, підтримку національного інформаційного простору, та гарантування конституційних прав громадян. Це потребує створення ефективної організаційно-правової бази, чітко визначених органів влади, відповідальних за інформаційну безпеку, та системи правових норм, що регулюють цю сферу.

Підвищення рівня медіакультури та медіаграмотності громадян, розвиток системи стратегічних комунікацій, та ефективна протидія дезінформації виступають ключовими елементами успішної національної стратегії інформаційної безпеки. Забезпечення технічної безпеки інформаційних систем, особливо у військовій сфері, є критично важливим для запобігання умисному пошкодженню систем або крадіжці конфіденційної інформації.

ЛІТЕРАТУРА:

1. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64 .URL : https://www.president.gov.ua/documents/642022-41397 (дата звернення 13.02.2024).

2. Конституція України від 28.06.1996. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/conv#Text (дата звернення 13.02.2024).

3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. : Закон України від 09 січня 2007 р. № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16?find=1&text=%E1%E5%E7%E. (дата звернення 13.02.2024).

4. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с

5. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал.* 2020. № 2. С. 200–203.

6. Косогов О.М., Сірик А.О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України. *Системи озброєння і військова техніка.* 2017. С. 38–41.

7. Гуржій Т. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право.* 2018. № 4. С. 16–26.

8. Під час війни кількість кібератак на Україну зросла втричі, – Мінфін США. URL: https://it.novyny.live/pid-chas-viini-kilkist-kiberatak-na-ukrayinu-zrosla-vtrichi-minfin-ssha-132751.html (дата звернення 13.02.2024).

9. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року : Розпорядження від 30 березня 2023 року. № 272-р. URL : https://ips.ligazakon.net/document/KR230272?an=1 (дата звернення 13.02.2024).